Chapter 1 System Overview 1-1

1.1 Introduction to Product 1-1
1.2 Service Functions..... 1-3
1.3 System Structure..... 1-4
1.3.1 Hardware Structure..... 1-4
1.3.2 Software Structure 1-5

Chapter 2 Installing Hardware 2-1

2.1 Installation Requirements..... 2-1
2.1.1 Attentions in Installation..... 2-1
2.1.2 Requirements for Installation Environment..... 2-2
2.1.3 Requirements for Electromagnetic Environment..... 2-2
2.1.4 Tools and Meters 2-3
2.2 Installing Hardware 2-4
2.2.1 Putting IAD108 on Desktop 2-4
2.2.2 Connecting Serial Port Cable 2-4
2.2.3 Connecting Uplink Cable 2-6
2.2.4 Connecting the Cable on User Side..... 2-8
2.2.5 Connecting Power Cable 2-9

Chapter 3 Loading Software 3-1

3.1 Setting up Configuration Environment for Loading 3-1

3.1.1 Setting up Configuration Environment for Loading through Local Serial Port 3-1
3.1.2 Setting up the Environment for Loading through Telnet..... 3-8
3.2 Updating Software..... 3-10
3.2.1 Configuring TFTP Server 3-10
3.2.2 Configuring FTP Server 3-13
3.3 Loading Software 3-17
3.3.1 BIOS Mode 3-17
3.3.2 Command Line Loading Mode... 3-28
Chapter 4 Configuring Data..... 4-1
4.1 Preparations Before Configuration 4-1
4.1.1 Collecting Data 4-1
4.1.2 Login Environment..... 4-3
4.2 Basic Commands 4-7
4.2.1 Command Modes 4-8
4.2.2 Usually Use Commands 4-10
4.2.3 Examples 4-11
4.3 Process of Data Configuration 4-12
4.4 Configuring Basic Data of the Equipment..... 4-13
4.4.1 Task List 4-13
4.4.2 Configuring the Data of This Equipment..... 4-15
4.4.3 Configuring IP Address of IAD108..... 4-19

4.4.4 Configuring System Time of IAD108 4-25
4.4.5 Starting DNS Client 4-28
4.4.6 Adding IADMS 4-29
4.5 Configuring MG Data 4-33
4.5.1 Task List 4-33
4.5.2 Configuring MG Registration Information 4-33
4.5.3 Configuring MG Attribute 4-35
4.6 Configuring Voice User Data 4-39
4.6.1 Configuring Ordinary Voice User 4-40
4.6.2 Configuring SPC Service 4-45
4.7 Configuration Examples of IAD108 4-51
4.7.1 Description of Networking 4-51
4.7.2 Collecting Data 4-53
4.7.3 Configuring Basic Information of IAD108 4-54
4.7.4 Configuring MG Attribute Data... 4-56
4.7.5 Configuring Voice User Data 4-58
4.7.6 Saving Configuration Data 4-61

Chapter 5 Advanced Configuration 5-1

5.1 Configuring Common Attributes of Access User 5-1
5.1.1 Configuring Ringing Mapping Record 5-1

5.1.2 Configuring PSTN Port Attribute 5-3
5.2 Configuring Parameters of Built- In LAN Switch 5-8
5.2.1 Configuring Precedence of Voice Packets 5-9
5.2.2 Other Configurations of LAN Switch 5-14
5.3 Configuring Software Parameters 5-18
5.3.1 Configuring System Software Parameters 5-18
5.3.2 Configuring MG Software Parameters 5-22
5.4 Configuring Standby MGC 5-24
5.5 Configuring MGCP Parameters 5-26
Chapter 6 ADSL Service Configuration 6-1
6.1 Creating Configuration Environment 6-1
6.1.1 CSP Hardware Version 6-1
6.1.2 ADSL Subboard 6-2
6.1.3 Connecting Uplink Interface 6-6
6.1.4 Connecting Downlink Interface 6-6
6.1.5 Example of Configuration Environment 6-7
6.2 ADSL Configuration Commands 6-8
6.2.1 ATM Related Commands 6-9
6.2.2 PPP Related Commands 6-10

6.2.3 EoA Related Commands 6-11
6.2.4 Bridging Related 6-11
6.3 Bridging Mode 6-12
6.3.1 Introduction to Bridging Principles 6-12
6.3.2 Networking Examples 6-13
6.3.3 Configuration Procedures 6-15
6.3.4 Configuration Examples 6-16

Chapter 7 Maintaining System 7-1

7.1 System Management 7-1
7.1.1 Saving Data 7-1
7.1.2 Rebooting the System 7-2
7.1.3 Showing CPU Occupancy 7-3
7.1.4 Showing System Date and Time 7-3
7.1.5 Showing Version Information 7-4
7.1.6 Controlling the Information Output to the Terminals 7-5
7.2 Access Service Management 7-11
7.2.1 Starting/Terminating Access Service 7-11
7.2.2 Resetting Access User Port 7-13
7.2.3 Showing Port Status 7-13
7.2.4 Showing Access User Data 7-14
7.2.5 Sending On-hook Signals to Console 7-15
7.3 Operator Management 7-16

7.3.1 Adding/Deleting Operator 7-17
7.3.2 Setting Operator Authority 7-19
7.3.3 Changing Operator's Password 7-20
7.3.4 Setting Reenter Number 7-21
7.3.5 Setting Operator's Appendix Information 7-22
7.3.6 Showing Operator's Information 7-23
7.3.7 Disconnecting Login Operator ... 7-25
7.4 Management of Operation Log 7-25
7.4.1 Adding Log host 7-27
7.4.2 Deleting Log Host 7-28
7.4.3 Activating Log Host 7-28
7.4.4 Deactivating Log Host 7-31
7.4.5 Showing Operation Log Information 7-33
7.4.6 Showing Operation Log List 7-34
7.4.7 Showing Log Host Configurations 7-37
7.4.8 Setting Information Output Control Switch of Log Host 7-38
7.4.9 Setting Information Output Control Level of Log Host 7-40
7.4.10 Querying Information Output Control Switch of Log Host 7-42
7.4.11 Showing Information Output Control Level of Log Host 7-43
7.5 Alarm Management 7-44

7.5.1 Description of Common Alarm Attributes 7-44
7.5.2 Alarm Management Task 7-46
7.5.3 Showing Alarm Records 7-47
7.5.4 Showing Alarm Configuration Information 7-52
7.5.5 Setting Alarm Output to Command Line Terminal 7-52
7.6 Setting RTCP Alarm Threshold 7-56
7.7 Patch Management 7-58
7.7.1 Overview of Patch 7-58
7.7.2 Steps of Operating Patches 7-59
7.8 Network Test Tools 7-60
7.8.1 ping 7-60
7.8.2 tracert 7-62
7.8.3 Example for Command Ping 7-63
7.8.4 Example for Command tracert ... 7-66

Chapter 8 Troubleshooting 8-1

8.1 Common Fault- locating Means 8-1
8.1.1 Showing Important System Information 8-1
8.1.2 Showing Alarms 8-5
8.1.3 Capturing Network Packets 8-7
8.1.4 Tracing Signaling 8-7
8.2 IAD Port ID Error Leads to Call Failure. 8-8
8.2.1 Symptom Description 8-8

8.2.2 Causal Analysis 8-8
8.2.3 Processing Procedure 8-9
8.2.4 Suggestion and Summary 8-10
8.3 Echo Occurs in PSTN Calls. 8-11
8.3.1 Fault 8-11
8.3.2 Cause 8-11
8.3.3 Processing Procedure 8-12
8.4 Call Fails After Telephone Ringing 8-12
8.4.1 Fault 8-12
8.4.2 Cause 8-12
8.4.3 Processing Procedure 8-13
8.5 Monolog 8-14
8.5.1 Fault 8-14
8.5.2 Cause 8-14
8.5.3 Processing Procedure 8-14
8.6 Voice Quality Deterioration 8-15
8.6.1 Fault 8-15
8.6.2 Cause 8-15
8.6.3 Processing Procedure 8-16
8.6.4 Suggestion and Summary 8-16
8.7 IAD Echo 8-16
8.7.1 Fault 8-16
8.7.2 Cause 8-17
8.7.3 Processing Procedure 8-17
8.8 Voice Abnormality 8-19
8.8.1 Fault 8-19

8.8.2 Cause 8-19
8.8.3 Processing Procedure 8-20

Appendix A Command List..... A-1

Appendix B Acronyms B-1

HUAWEI

U-SYS IAD108 Integrated Access Device

User Manual

V200R002

U-SYS IAD108 Integrated Access Device

User Manual

Manual Version T2-010131-20041015-C-2.20

Product Version V200R002

BOM 31013731

Huawei Technologies Co., Ltd. provides customers with comprehensive technical support and service. Please feel free to contact our local office or company headquarters.

Huawei Technologies Co., Ltd.

Address: Administration Building, Huawei Technologies Co., Ltd.,

Bantian, Longgang District, Shenzhen, P. R. China

Postal Code: 518129

Website: http://www.huawei.com

Email: support@huawei.com

Copyright © 2004 Huawei Technologies Co., Ltd.

All Rights Reserved

No part of this manual may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks

, HUAWEI, C&C08, EAST8000, HONET, , ViewPoint, INtess, ETS, DMC, TELLIN, InfoLink, Netkey, Quidway, SYNLOCK, Radium, M900/M1800, TELESIGHT, Quidview, Musa, Airbridge, Tellwin, Inmedia, VRP, DOPRA, iTELLIN, HUAWEI OptiX, C&C08 iNET, NETENGINE, OptiX, iSite, U-SYS, iMUSE, OpenEye, Lansway, SmartAX, infoX, TopEng are trademarks of Huawei Technologies Co., Ltd.

All other trademarks mentioned in this manual are the property of their respective holders.

Notice

The information in this manual is subject to change without notice. Every effort has been made in the preparation of this manual to ensure accuracy of the contents, but all statements, information, and recommendations in this manual do not constitute the warranty of any kind, express or implied.

About This Manual

Release Notes

The product version that corresponds to the manual is U-SYS IAD108 Integrated Access Device V200R002.

Organization

The manual introduces the functions and operations of the U-SYS IAD108 Integrated Access Device.

There are 8 chapters and 2 appendixes in the manual.

Chapter 1 System Overview profiles the system characteristics, main functions, system structure, and external interfaces of the IAD108.

Chapter 2 Installing Hardware introduces how to install the hardware of IAD108.

Chapter 3 Loading Software elaborates on the establishing of configuration environment and how to load the software.

Chapter 4 Configuring Data presents how to configure various data needed for providing various services.

Chapter 5 Advanced Configuration introduces various advanced configurations related to IAD108 when cooperating with other devices.

Chapter 6 ADSL Service Configuration introduces how to configure ADSL services.

Chapter 7 Maintaining System introduces how to maintain the system.

Chapter 8 Troubleshooting introduces how to locate and remove the faults of the system.

Appendix A Command List lists all the commands used for configuring IAD108 in alphabetic order.

Appendix B Acronyms lists all the acronyms appeared in the manual.

Intended Audience

The manual is intended for the following readers:

- Installation engineers and technicians
- Operation and maintenance personnel

Conventions

The manual uses the following conventions:

I. General conventions

Convention	Description
Arial	Normal paragraphs are in Arial.
Arial Narrow	Warnings, Cautions, Notes and Tips are in Arial Narrow.

Boldface	Headings are in **Boldface**.
`Courier New`	Terminal Display is in `Courier New`.

II. Command conventions

Convention	Description
Boldface	The keywords of a command line are in **Boldface**.
italic	Command arguments are in *italic*.
[ ]	Items (keywords or arguments) in square brackets [ ] are optional.
{ x | y | ... }	Alternative items are grouped in braces and separated by vertical bars. One is selected.
[x | y | ...]	Optional alternative items are grouped in square brackets and separated by vertical bars. One or none is selected.
{ x | y | ... } *	Alternative items are grouped in braces and separated by vertical bars. A minimum of one or a maximum of all can be selected.
[x | y | ...] *	Optional alternative items are grouped in square brackets and separated by vertical bars. Many or none can be selected.

III. GUI conventions

Convention	Description
< >	Button names are inside angle brackets. For example, click the <OK> button.
[ ]	Window names, menu items, data table and field

Convention	Description
	names are inside square brackets. For example, pop up the [New User] window.
/	Multi-level menus are separated by forward slashes. For example, [File/Create/Folder].

IV. Keyboard operation

Format	Description
<Key>	Press the key with the key name inside angle brackets. For example, <Enter>, <Tab>, <Backspace>, or <A>.
<Key1+Key2>	Press the keys concurrently. For example, <Ctrl+Alt+A> means the three keys should be pressed concurrently.
<Key1, Key2>	Press the keys in turn. For example, <Alt, A> means the two keys should be pressed in turn.

V. Mouse operation

Action	Description
Click	Press the left button or right button quickly (left button by default).
Double Click	Press the left button twice continuously and quickly.
Drag	Press and hold the left button and drag it to a certain position.

VI. Symbols

Eye-catching symbols are also used in this manual to highlight the points worthy of special attention during the operation. They are defined as follows:

⚠ **Caution**, **Warning**, **Danger**: Means reader be extremely careful during the operation.

🕮 **Note**, **Comment**, **Tip**, **Knowhow**, **Thought**: Means a complementary description.

Environmental Protection

This product has been designed to comply with the requirements on environmental protection. For the proper storage, use and disposal of this product, national laws and regulations must be observed.

Table of Contents

Chapter 1 System Overview 1-1
1.1 Introduction to Product 1-1
1.2 Service Functions 1-3
1.3 System Structure 1-4
1.3.1 Hardware Structure 1-4
1.3.2 Software Structure 1-5

Chapter 2 Installing Hardware 2-1
2.1 Installation Requirements 2-1
2.1.1 Attentions in Installation 2-1
2.1.2 Requirements for Installation Environment 2-2
2.1.3 Requirements for Electromagnetic Environment 2-2
2.1.4 Tools and Meters 2-3
2.2 Installing Hardware 2-4
2.2.1 Putting IAD108 on Desktop 2-4
2.2.2 Connecting Serial Port Cable 2-4
2.2.3 Connecting Uplink Cable 2-6
2.2.4 Connecting the Cable on User Side 2-8
2.2.5 Connecting Power Cable 2-9

Chapter 3 Loading Software 3-1
3.1 Setting up Configuration Environment for Loading 3-1
3.1.1 Setting up Configuration Environment for Loading through Local Serial Port 3-1
3.1.2 Setting up the Environment for Loading through Telnet 3-8

3.2 Updating Software....3-10
3.2.1 Configuring TFTP Server....3-10
3.2.2 Configuring FTP Server....3-13
3.3 Loading Software....3-17
3.3.1 BIOS Mode....3-17
3.3.2 Command Line Loading Mode....3-28

Chapter 4 Configuring Data....4-1
4.1 Preparations Before Configuration....4-1
4.1.1 Collecting Data....4-1
4.1.2 Login Environment....4-3
4.2 Basic Commands....4-7
4.2.1 Command Modes....4-8
4.2.2 Usually Use Commands....4-10
4.2.3 Examples....4-11
4.3 Process of Data Configuration....4-12
4.4 Configuring Basic Data of the Equipment....4-13
4.4.1 Task List....4-13
4.4.2 Configuring the Data of This Equipment....4-15
4.4.3 Configuring IP Address of IAD108....4-19
4.4.4 Configuring System Time of IAD108....4-25
4.4.5 Starting DNS Client....4-28
4.4.6 Adding IADMS....4-29
4.5 Configuring MG Data....4-33
4.5.1 Task List....4-33
4.5.2 Configuring MG Registration Information....4-33
4.5.3 Configuring MG Attribute....4-35
4.6 Configuring Voice User Data....4-39
4.6.1 Configuring Ordinary Voice User....4-40
4.6.2 Configuring SPC Service....4-45

4.7 Configuration Examples of IAD108 4-51
4.7.1 Description of Networking 4-51
4.7.2 Collecting Data 4-53
4.7.3 Configuring Basic Information of IAD108 4-54
4.7.4 Configuring MG Attribute Data 4-56
4.7.5 Configuring Voice User Data 4-58
4.7.6 Saving Configuration Data 4-61

Chapter 5 Advanced Configuration 5-1
5.1 Configuring Common Attributes of Access User 5-1
5.1.1 Configuring Ringing Mapping Record 5-1
5.1.2 Configuring PSTN Port Attribute 5-3
5.2 Configuring Parameters of Built-In LAN Switch 5-8
5.2.1 Configuring Precedence of Voice Packets 5-9
5.2.2 Other Configurations of LAN Switch 5-14
5.3 Configuring Software Parameters 5-18
5.3.1 Configuring System Software Parameters 5-18
5.3.2 Configuring MG Software Parameters 5-22
5.4 Configuring Standby MGC 5-24
5.5 Configuring MGCP Parameters 5-26

Chapter 6 ADSL Service Configuration 6-1
6.1 Creating Configuration Environment 6-1
6.1.1 CSP Hardware Version 6-1
6.1.2 ADSL Subboard 6-2
6.1.3 Connecting Uplink Interface 6-6
6.1.4 Connecting Downlink Interface 6-6
6.1.5 Example of Configuration Environment 6-7
6.2 ADSL Configuration Commands 6-8
6.2.1 ATM Related Commands 6-9
6.2.2 PPP Related Commands 6-10

6.2.3 EoA Related Commands 6-11
6.2.4 Bridging Related 6-11
6.3 Bridging Mode 6-12
6.3.1 Introduction to Bridging Principles 6-12
6.3.2 Networking Examples 6-13
6.3.3 Configuration Procedures 6-15
6.3.4 Configuration Examples 6-16

Chapter 7 Maintaining System 7-1
7.1 System Management 7-1
7.1.1 Saving Data 7-1
7.1.2 Rebooting the System 7-2
7.1.3 Showing CPU Occupancy 7-3
7.1.4 Showing System Date and Time 7-3
7.1.5 Showing Version Information 7-4
7.1.6 Controlling the Information Output to the Terminals 7-5
7.2 Access Service Management 7-11
7.2.1 Starting/Terminating Access Service 7-11
7.2.2 Resetting Access User Port 7-13
7.2.3 Showing Port Status 7-13
7.2.4 Showing Access User Data 7-14
7.2.5 Sending On-hook Signals to Console 7-15
7.3 Operator Management 7-16
7.3.1 Adding/Deleting Operator 7-17
7.3.2 Setting Operator Authority 7-19
7.3.3 Changing Operator's Password 7-20
7.3.4 Setting Reenter Number 7-21
7.3.5 Setting Operator's Appendix Information 7-22
7.3.6 Showing Operator's Information 7-23
7.3.7 Disconnecting Login Operator 7-25

7.4 Management of Operation Log 7-25
7.4.1 Adding Log host.....7-27
7.4.2 Deleting Log Host 7-28
7.4.3 Activating Log Host.....7-28
7.4.4 Deactivating Log Host 7-31
7.4.5 Showing Operation Log Information.....7-33
7.4.6 Showing Operation Log List 7-34
7.4.7 Showing Log Host Configurations 7-37
7.4.8 Setting Information Output Control Switch of Log Host7-38
7.4.9 Setting Information Output Control Level of Log Host7-40
7.4.10 Querying Information Output Control Switch of Log Host 7-42
7.4.11 Showing Information Output Control Level of Log Host 7-43
7.5 Alarm Management.....7-44
7.5.1 Description of Common Alarm Attributes 7-44
7.5.2 Alarm Management Task 7-46
7.5.3 Showing Alarm Records.....7-47
7.5.4 Showing Alarm Configuration Information.....7-52
7.5.5 Setting Alarm Output to Command Line Terminal 7-52
7.6 Setting RTCP Alarm Threshold.....7-56
7.7 Patch Management 7-58
7.7.1 Overview of Patch 7-58
7.7.2 Steps of Operating Patches 7-59
7.8 Network Test Tools 7-60
7.8.1 ping.....7-60
7.8.2 tracert 7-62
7.8.3 Example for Command Ping 7-63
7.8.4 Example for Command tracert 7-66

Chapter 8 Troubleshooting **8-1**
8.1 Common Fault-locating Means 8-1
8.1.1 Showing Important System Information 8-1
8.1.2 Showing Alarms 8-5
8.1.3 Capturing Network Packets 8-7
8.1.4 Tracing Signaling 8-7
8.2 IAD Port ID Error Leads to Call Failure. 8-8
8.2.1 Symptom Description 8-8
8.2.2 Causal Analysis 8-8
8.2.3 Processing Procedure 8-9
8.2.4 Suggestion and Summary 8-10
8.3 Echo Occurs in PSTN Calls. 8-11
8.3.1 Fault 8-11
8.3.2 Cause 8-11
8.3.3 Processing Procedure 8-12
8.4 Call Fails After Telephone Ringing 8-12
8.4.1 Fault 8-12
8.4.2 Cause 8-12
8.4.3 Processing Procedure 8-13
8.5 Monolog 8-14
8.5.1 Fault 8-14
8.5.2 Cause 8-14
8.5.3 Processing Procedure 8-14
8.6 Voice Quality Deterioration 8-15
8.6.1 Fault 8-15
8.6.2 Cause 8-15
8.6.3 Processing Procedure 8-16
8.6.4 Suggestion and Summary 8-16
8.7 IAD Echo 8-16

8.7.1 Fault....8-16
8.7.2 Cause....8-17
8.7.3 Processing Procedure....8-17
8.8 Voice Abnormality....8-19
8.8.1 Fault....8-19
8.8.2 Cause....8-19
8.8.3 Processing Procedure....8-20

Appendix A Command List....A-1

Appendix B Acronyms....B-1

Chapter 1 System Overview

1.1 Introduction to Product

Integrated Access Device (IAD) is an important component of the Next Generation Network (NGN).

Huawei's IAD108 is an Access Media Gateway (AMG) based on the technologies of Voice over IP (VoIP) and Fax over IP (FoIP). It not only provides efficient and excellent voice services on the world-wide IP network (the Internet or Intranet), and also provides small-capacity VoIP/FoIP solutions for enterprises, users in communities and companies.

IAD108 adopts the box design, and is usually installed on the desktops or hung in the corridors. The appearance is as shown in Figure 1-1.

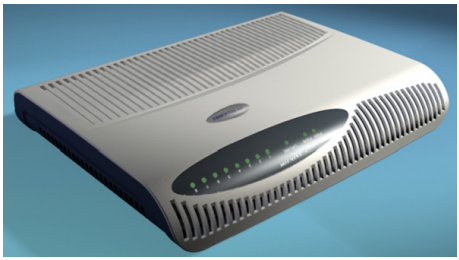


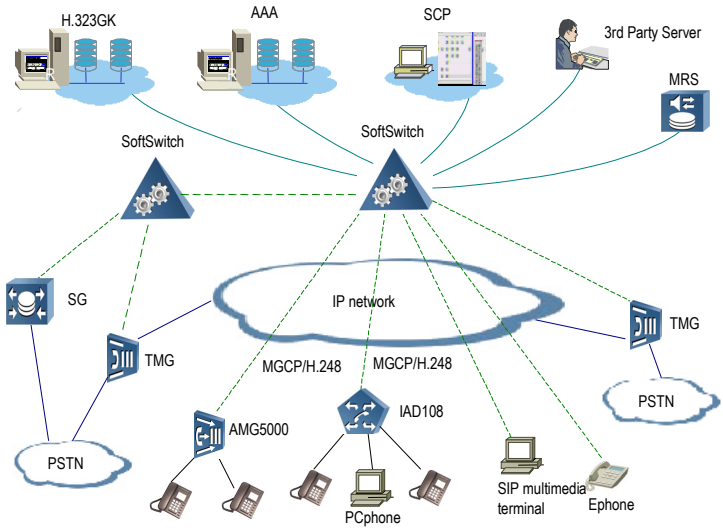
Figure 1-1 Appearance of IAD108

According to different uplink interfaces, IAD108 series include three models as listed in Table 1-1.

Table 1-1 Three models of IAD108 series

Model	Uplink interface
IAD108A	The uplink interface type is asymmetric digital subscriber line (ADSL).
IAD108E	The uplink interface type is fast Ethernet (FE).
IAD108V	The uplink interface type is very-high-data-rate digital subscriber line (VDSL).

IAD108 is located in the user access level of NGN, as shown in Figure 1-2.



AAA: Authentication, Authorization and Accounting
SCP: Service Control Point
MRS: Media Resource Server
SG: Signaling Gateway
TMG: Trunk Media Gateway
AMG: Access Media Gateway

Figure 1-2 Location of IAD108 in NGN

1.2 Service Functions

Acting as a device in the user access layer of NGN, IAD108 can provide abundant services:

- Access POTS users to IP network.
- Access Ethernet users into IP packet network.
- Support IP semi-permanent connection (SPC) and internal SPC.
- Support T.38 fax or transparent transmission of fax.
- Support transparent transmission of Modem signals.

- Test on subscriber line. (optional)
- Support the power supply from remote place.
- Support traditional PSTN telephone services, including: call forwarding, Caller Identification Display (CID) and call waiting. With the right telephone set, voice message indicator function can also be provided.
- Support the supplementary services in coordination with a softswitch.
- Support intelligent services and special applications in coordination with a softswitch.

1.3 System Structure

1.3.1 Hardware Structure

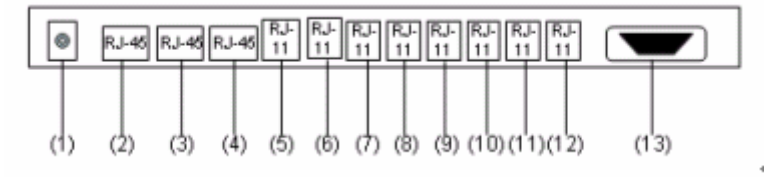
There are indicators on the front panel of IAD108, and their names and meanings are as shown in Table 1-2.

Table 1-2 Table of IAD108 indicators

Indicator	Color	Name	Meaning
PWR	Green	Power supply indicator	When local power supply is connected, it is on. If there is no power supply, it is off. When remote power supply is connected, it blinks. If there is no power supply, it is off.
RUN	Green	Running indicator	It blinks two times per second when loading. It blinks one time per second when running normally.

Indicator	Color	Name	Meaning
WAN	Green	Indicator for uplink interface	When the unplink interface is normal, it is on, and if no network cable is inserted, it is off.
1–8	Green	Indicator for telephone user	When the user on the corresponding interface off-hooks, it is lighted up.

The external interfaces provided by IAD108 are located on the back panel as shown in Figure 1-3.



(1) Local power supply interface (2) Upstream interface (3), (4) Data user interface
(5)–(12) POTS ports (13) Local maintenance serial port

Figure 1-3 External interface of IAD108

1.3.2 Software Structure

The software system of IAD108 consists of the main CPU software and DSP software of the CSP. As the core of IAD, the main CPU software implements the call control of the whole system, management and maintenance function and forwarding of media flow. The DSP software mainly implements the coding and decoding of voice, detection and generation of Dual-tone Multifrequency

(DTMF)/ Frequency Shift Keying (FSK), Voice Activity Detection (VAD) and Comfort Noise Generation (CNG).

In terms of software structure, IAD108 consists of the following functionality modules.

- Management, maintenance and operation system module
- Service access module
- SPC service processing module
- VoIP service processing module
- Protocol processing module
- Bottom layer drive module

The relations among the modules are shown in Figure 1-4.

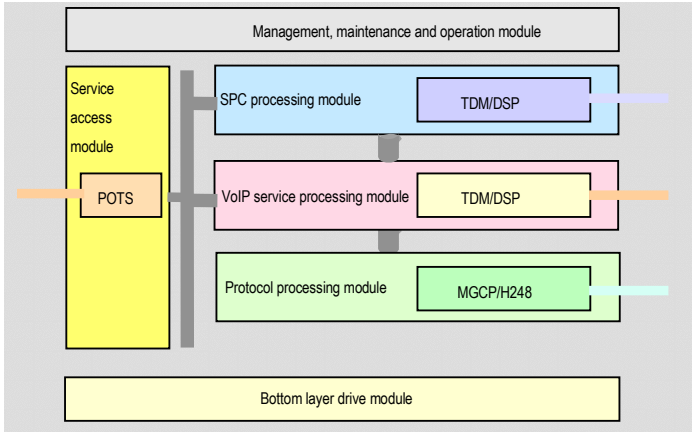


Figure 1-4 Functionality modules of IAD108

The functions of these modules are listed in Table 1-3.

Table 1-3 Functions of modules in IAD108

Module	Function
Management, maintenance and operation module	It is responsible for maintenance, operation and management of the whole IAD108 system.
Service access module	It implements the selection, summary and report of analog user and digital user information, and transmits the messages issued by the service module.
SPC service processing module	It establishes and maintains the SPCs between the different users in the same IAD108, or different users in different IAD108s.
VoIP service processing module	It controls the interaction of user signalings and the Time Division Multiplexing (TDM)/ Digital Signal Processing (DSP) user module, and implements the interconnection with the Media Gateway Controller (MGC).
Protocol processing module	It implements the processing of MGCP/H248 protocol stack and the adaptation of protocols.
Bottom layer drive module	It drives various function chips on the CSP.

Chapter 2 Installing Hardware

IAD108 consists of hardware system and software system. Before running the equipment, you must install the hardware and load the software.

2.1 Installation Requirements

2.1.1 Attentions in Installation

To avoid the damaged to equipment or the hurt to human body caused by improper operation, you should pay attention to the items listed in Table 2-1.

Table 2-1 Attentions in installation

Item	Description
1	Do not put the equipment beside water or in damp place, in order to prevent water and moisture from entering the equipment.
2	Do not put the equipment on precarious box or desk, in case it falls, it will be seriously damaged.
3	Make sure that the working voltage is the same as the rated voltage, because IAD108 can only work normally at proper voltage.
4	Never open the shell when the device is working. Do not open the shell, even if it is powered off, unless absolutely necessary.
5	Before cleaning IAD108, pull out the power plug of the device. Wipe IAD108 with dry cloths, and do not wash IAD108 with any liquid.

2.1.2 Requirements for Installation Environment

IAD108 must be installed indoors. No matter it is installed in the corridor or put on the desktop, the following conditions must be guaranteed.

- Make sure that enough spaces are reserved for the inlet and outlet of IAD108 to facilitate heat dissipation.
- Make sure that the corridor and the desktop is well ventilated.
- The working temperature of IAD108 is -5 to 50 degrees Celsius, and the environmental humidity is 10%–90%.

2.1.3 Requirements for Electromagnetic Environment

IAD108 may be influenced by external electromagnetic signals in radiation mode or conductive mode during its operation. Therefore, you should pay attention to the points listed in Table 2-2.

Table 2-2 Measures for preventing electromagnetic interference

Item	Description
1	AC power receptacles should be monophase three-wire receptacles with protection grounding (PE). So that the filtration circuit on the equipment can effectively filter the interference from electricity power supply.
2	The work site of the equipment should be far from powerful radio station, radar station, or devices with high-frequency or huge-current.
3	If necessary, Electromagnetic masking method can be adopted, such as adopting making cables for interface cables.

Item	Description
4	The interface cables must be wired indoors, and wiring them outdoors is prohibited, because the overvoltage and over-currrent caused by lightning will damage the signal interface.

2.1.4 Tools and Meters

The following meters and tools should be ready before the installation work is started:

Table 2-3 List of tools and meters

Universal tools	**Fastening tools**	Cross screwdriver M3
	Fitter tools	Sharp-nose pliers, diagonal pliers, pliers
Special tools	cable peeler, crimping pliers, and wire punch-down tool	
Meters	Multimeters, 500V megaohm meters (for measuring the insulation resistance)	

Note:

- The supplier should provide the list of tools and meters, and decide the provider of the tools and meters together with the customer.
- The meters must be calibrated and proved to be qualified before they can be used.

2.2 Installing Hardware

IAD108 is a box-like device with fixed configuration. Installation on site is very simple, and the main installation steps are connections of cables, as shown in Table 2-4

Table 2-4 Steps for installing hardware

Steps	Operation
1	Fixing IAD108 box onto the specified location.
2	Connecting serial port cable (optional).
3	Connecting upstream cable.
4	Connecting user side cable
5	Connecting power cable

2.2.1 Putting IAD108 on Desktop

Put IAD108 on a clean desktop. Such installation is very simple, and you should pay attention to the following:

- Make sure that the desktop is stable.
- Keep 10cm spaces around IAD108 for heat dissipation.
- Do not put heavy objects over IAD108.

2.2.2 Connecting Serial Port Cable

The serial port of IAD108 is the female DCE (Data Circuit-terminal Equipment) RS-232 port, as shown in Figure 2-1.

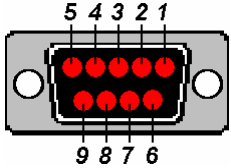


Figure 2-1 Serial port of IAD108

The serial port is on the right part of the device's rear panel. It is labeled as CONSOLE. Features of serial port are: transmission rate of 9600 bit/s, without parity check, 8 data bits, one stop bit, without traffic control.

The signals tranceived by pinouts are as shown in Table 2-5, and other unlisted pinouts are not used.

Table 2-5 Pingouts of the connector on console

Pingout	Signal	Sourcing from
2	TXD (transmit data)	DCE
3	RXD (receive data)	DTE (Data Terminal Equipment)
5	Grounding of signal	

IAD108 is connected with the maintenance terminal via a serial port cable. The delivered serial port cable can connect DB-9 male connector to DB-9 female connector. If the serial port on the maintenance terminal is not a DB-9 male connector, you should prepare the serial port cable by yourself.

The steps for connecting the serial port cable are as follows:

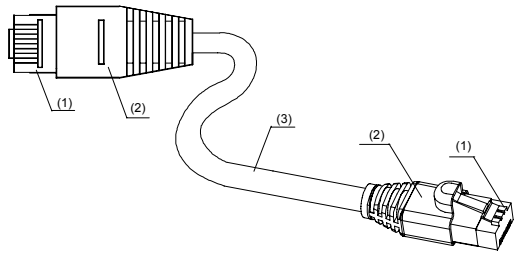
1) Connect female end of the serial port cable to the DB-9 male connector on the PC or terminal that will configure the IAD108.
2) Connect the DB-9 male connector of the serial port cable to the configuration port of IAD108.

2.2.3 Connecting Uplink Cable

Due to different uplink modes, IAD108 has three models: IAD108A, IAD108E and IAD108V correspond to ADSL uplink, Ethernet uplink and VDSL uplink. The cable connections of them are introduced. The connection methods for ADSL cable and VDSL cable are the same and will be introduced together.

I. IAD108E

IAD108E provides one channel of Fast Ethernet (FE) uplink, and the uplink cable is a straight-through cable, which consists of two RJ-45 connectors and a piece of category 5 cable. The appearance of straight-through cable is as shown in Figure 2-2.



(1): Crystal connector (2): Protection sheath (3): Category 5 cable

Figure 2-2 Connection of network cable

The structure of straight-through cable is as shown in Figure 2-3.

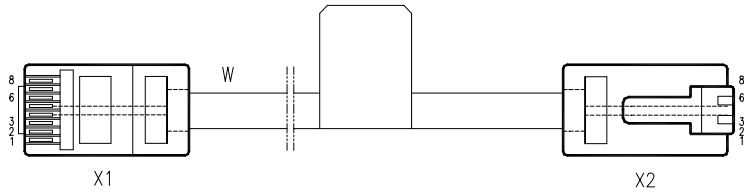


Figure 2-3 Structure of straight-through cable

The cable connections in straight-through cable are listed in Table 2-6.

Table 2-6 Cable connections in straight-through cable

Connector	8-core category 5 twisted pair cable	Connector
Pin 1	White (orange)	Pin 1
Pin 2	Orange	Pin 2
Pin 3	White (green)	Pin 3
Pin 4	Blue	Pin 4
Pin 5	White (blue)	Pin 5
Pin 6	Green	Pin 6
Pin 7	White (brown)	Pin 7
Pin 8	Brown	Pin 8

IAD108E uses a straight-through cable to connect the upper network device. The connection steps are as follows:

1) Insert one end of the network cable into the uplink interface (the RJ-45 interface close to the power interface) on the back panel of IAD108E. Align the strip to the gap on the interface and insert the RJ-45 connector. If a “click” is heard, the connector is well plugged.
2) Connect the other end of the network cable to the uplink network device according to actual situations.

II. IAD108A/IAD108V

IAD108A/IAD108V provides one channel of ADSL/VDSL uplink, and the uplink interface is the RJ-45 port beside the power interface. ADSL/VDSL cable is an ordinary telephone line. The connection steps are as follows:

1) Insert the RJ-11 connector of the telephone line into the uplink RJ-45 interface on the IAD108A/IAD108V.
2) Connect the other end of the telephone line to the uplink Digital Subscriber Line Access Multiplexer (DSLAM) device.

2.2.4 Connecting the Cable on User Side

There are two kinds of subscriber cables: RJ-11 telephone line and RJ-45 straight-through cable. They are used to connect different types of subscriber interfaces. The correlation between the subscriber interfaces and cables are as follows:

- POTS port: There are eight POTS ports on the rear panel, which can be connected with RJ-11 telephone line.

- Network interface: There are two downlink interfaces, which can be connected with straight-through cables.

I. Connecting Ordinary Telehphone Cables

Insert one end of the cable into an RJ-11 user interface, and the other end into the socket on the telephone set.

II. Connecting Straight-through Network Cable

1) Insert one end of the network cable into the downstream RJ-45 interface on the back panel of IAD108. Align the strip to the gap on the interface and insert the RJ-45 connector. If a “click” is heard, the connector is well plugged.
2) Insert the other end of the network cable into the interface on the network adapter of the PC. If the LINK indicators on both IAD108 and the PC are lighted, it means the network cable is correctly connected.

2.2.5 Connecting Power Cable

Usually, IAD108 adopts local 12V power as working power. If IAD108 uplinks via FE, and the upper device (like LAN Switch) supports remote power supply, IAD108 can also be powered by remote power supply, that means the IAD108 is powered by the upper device.

Caution:

It is recommended that IAD108E mainly uses local power supply and the remote power supply can be taken as emergency power supply.
To ensure safe operation, you must power on IAD108 after all the other cables have been installed and the installation check has been passed.

I. Connecting Local Power Supply

The local power supply of IAD208 is provided by the AC-DC adapter.

The input voltage range is AC 100–240V, input current is 1.0A, and input frequency is 50-60Hz. The DC output voltage is 12V, the peak output current is 3A, and the peak power is 36W.

Steps for connecting power cables

1) Check whether all the serial port cable, uplink cable and user cable have been correctly connected. If yes, the equipment can be powered on.
2) Insert the output end of AC-DC power cable into the power socket on the back panel of IAD108, and the other end into the external AC power socket.
3) Check whether the power indicator (PWR) on the front panel is normal. When the local power supply is used, the PWR indicator on the front panel is lighted.

Note:

It is recommended to use the monophase three-wire receptacles or multipurpose receptacles for PCs. The neutral pole of the power supply must be grounded reliably in the building. Generally, the neutral point of the power supply in a building should have already been grounded. However, remember to confirm this before you install IAD108.

II. Connecting Remote Power Supply

Remote power supply can power IAD108E through its uplink cable. IAD108E uses straight-through cable to uplink, and for the details of straight-through cable, refer to section 2.2.3 I. of this chapter.

When the remote power supply is correctly connected, the PWR indicator will flash at the frequency of 4 Hz.

Chapter 3 Loading Software

This chapter introduces how to load software after the hardware has been correctly installed.

For IAD108, loading means to write the programs and data files that are needed by the normal running of equipment into Flash memory, so as to ensure the system can be upgraded and run normally.

3.1 Setting up Configuration Environment for Loading

IAD108 can be loaded with software through local serial port or Telnet mode.

3.1.1 Setting up Configuration Environment for Loading through Local Serial Port

You can use the HyperTerminal software of Windows 98/2000/NT/XP to implement maintenance through the local serial port.

The connection between local serial port and the maintenance terminal (PC) is as shown in Figure 3-1. The serial port cable should already be connected when you are installing hardware. Refer to Chapter 2.

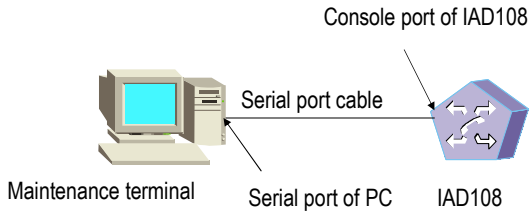


Figure 3-1 Connection for configuring through local serial port

The following is an example to connect and configure the local serial port terminal, which is an ordinary PC running Window98 operating system.

1) On the maintenance terminal, click [Start/Programs/Accessories/Communication/HyperTerminal], and then double click the “HyperTerminal” icon to start the HyperTerminal.
2) Input the name in the “Connection Description” dialog box like “IAD”, and click <OK> to establish the corresponding serial port connection, as shown in Figure 3-2. Then click <OK>.

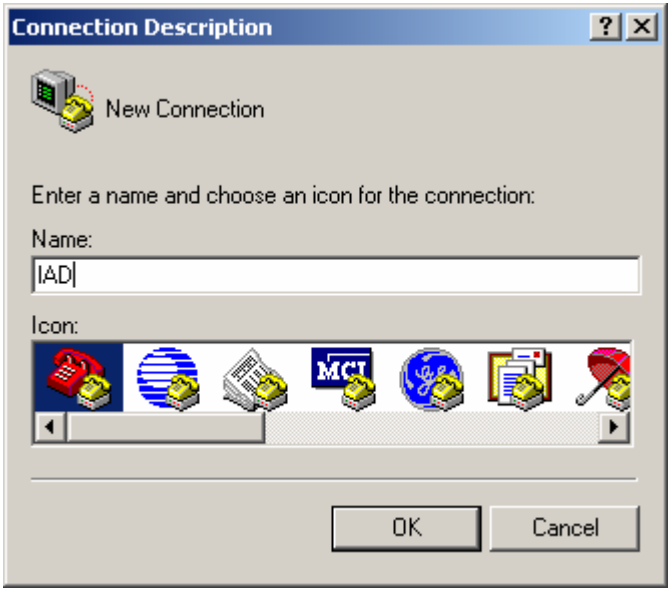


Figure 3-2 Set up a HyperTerminal connection

3) In the “Connect using” text box, select the actually used serial port number, like “Com1”, as shown in Figure 3-3. Then click <OK>.

Figure 3-3 Select the serial port number

4) Set the parameters of serial port: baud rate as 9600 bit/s (it must be consistent with that configured on IAD108 serial port, and the default value is 9600 bit/s), data bit as 8, 1 stop bit, without parity check and flow control. The settings are shown in Figure 3-4.

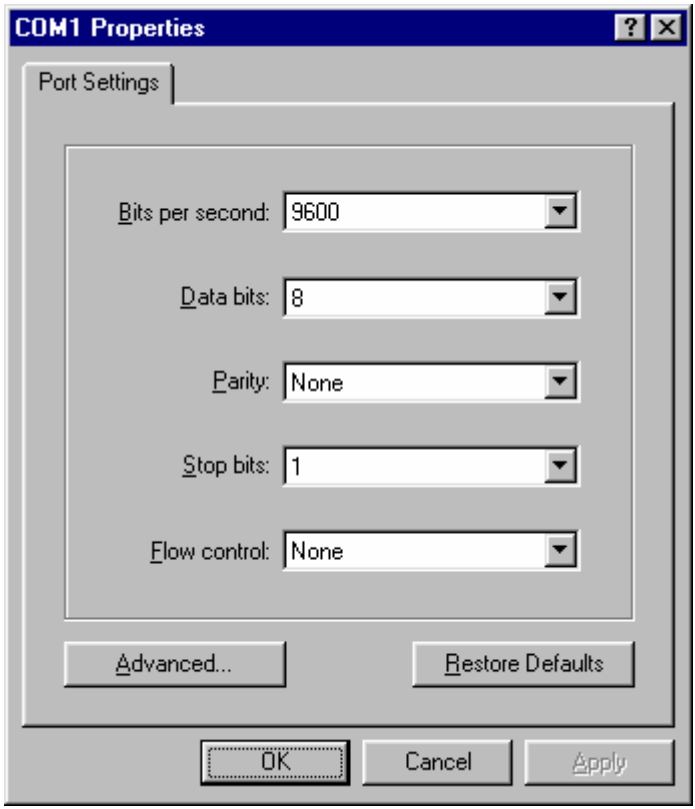


Figure 3-4 Set the properties for COM 1

5) Select the [File/Properties/Settings] menu in the HyperTerminal window, and set the Telnet terminal and emulation types as "ANSI" and "Auto Detect". Refer to Figure 3-5.

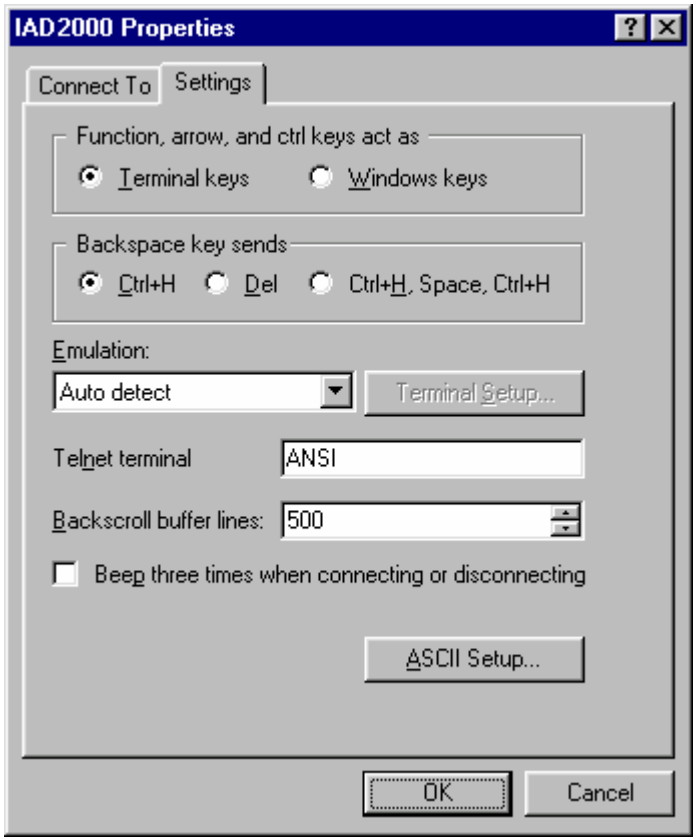


Figure 3-5 Set the properties of IAD108

6) Click the <ASCII Setup> button, set the "Line delay" and "Character delay" of the "ASCII sending" as 50ms, as shown in Figure 3-6.

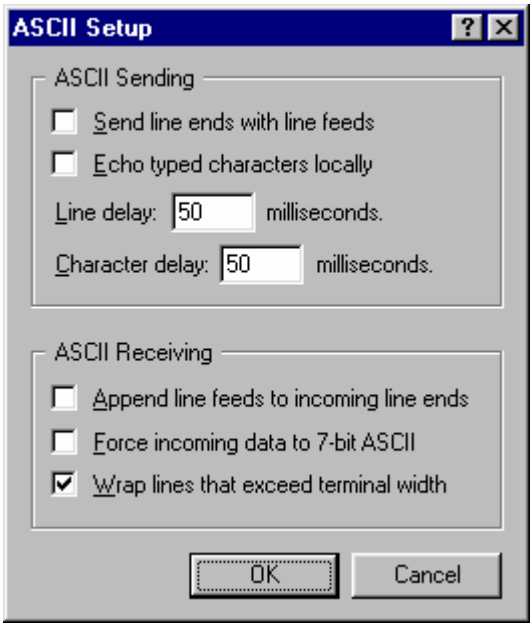


Figure 3-6 Set ASCII

Note:

"Character delay" controls the display speed of each character when the HyperTerminal shows text contents. "Line delay" controls the display time interval between two lines.

When the delay is too short, it may result in character loss. So if the display is abnormal, you should check the two values, and make modification if necessary.

---

7) After setting up the HyperTerminal, press <Enter> and the welcome interface of IAD108 will be shown on the terminal. Input the user name and password, then you can log in the equipment to operate and maintain the equipment.

3.1.2 Setting up the Environment for Loading through Telnet

To remotely load software through Telnet, ensure that IP attributes (like IP address, subnet mask, default gateway) of IAD108 have been correctly configured through local serial port.

The networking for maintaining IAD108 through Telnet is as shown in Figure 3-7.

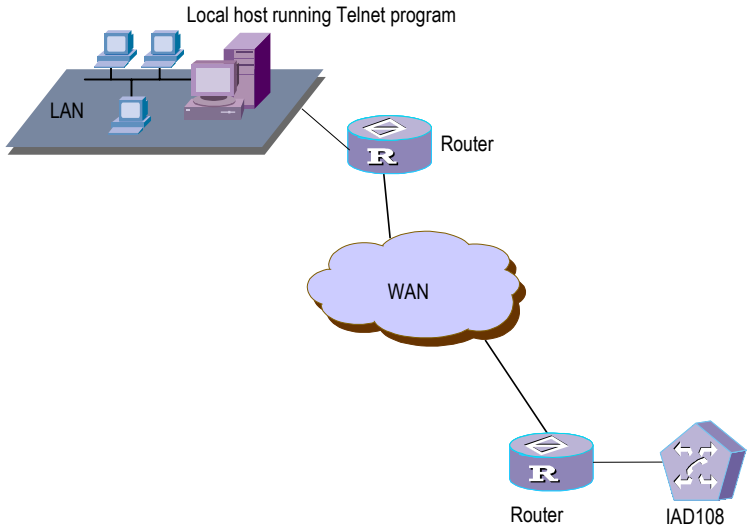


Figure 3-7 Set up Telnet connection for remote loading through a WAN

Configuration steps are as follows.

1) Run Telnet program on the maintenance terminal, set its terminal type as VT-100/ANSI and the buffer size as 1000, as shown in Figure 3-8.

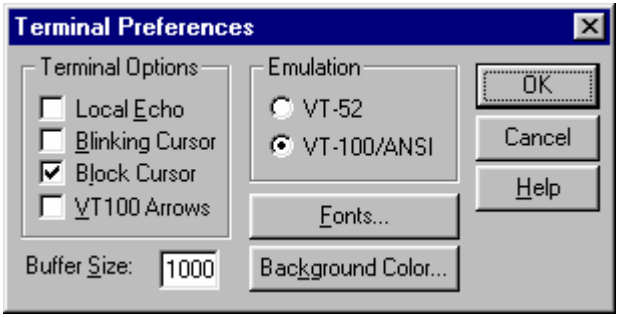


Figure 3-8 Set Telnet terminal preferences

Note:

The default Telnet buffer size is small, and you can increase the buffer size properly so that more history commands can be displayed on the screen. Recommended buffer size is 1000 lines.

2) Enter the IP address “172.21.100.16” of IAD108 on the maintenance terminal, and then establish the connection.
3) After connecting IAD108, input correct user name and password to log in the equipment to load software or configure data.

Note:

- When you are configuring IAD108 through Telnet, do not randomly change the IP address of IAD108. If it is necessary to modify the IP address, after the modification, the Telnet connection will be disconnected and you must log in again with the new IP address to establish the connection.
- The system allows 4 Telnet users to log in concurrently. If it prompts that there are too many users, you should wait and log in latter.

3.2 Updating Software

The loading of software can be made through Trivial File Transfer Protocol (TFTP) or File Transfer Protocol (FTP). If the IAD is not directly connected with the server which stores the load files, FTP mode is recommended, because the FTP transmission has higher reliability.

3.2.1 Configuring TFTP Server

When TFTP is used to update IAD108 software, the new software is downloaded through network interface. To do this, a PC is used as the file server to run TFTP server program.

Specific methods for configuring TFTP server.

1) Establish the TFTP server environment

First, take a PC as the TFTP server. Connect the TFTP server and IAD108 through network interfaces, and configure the IP address of TFTP server so that the two can ping each other.

2) Run TFTP program.

Note:

In this manual, TFTPD32 is taken as an example to demonstrate how to configure the TFTP server on this computer. The installation program of TFTP server is not delivered with the equipment, and you must get it by yourself.

Run TFTP program “TFTPD32”, and the interface after startup is as shown in Figure 3-9.

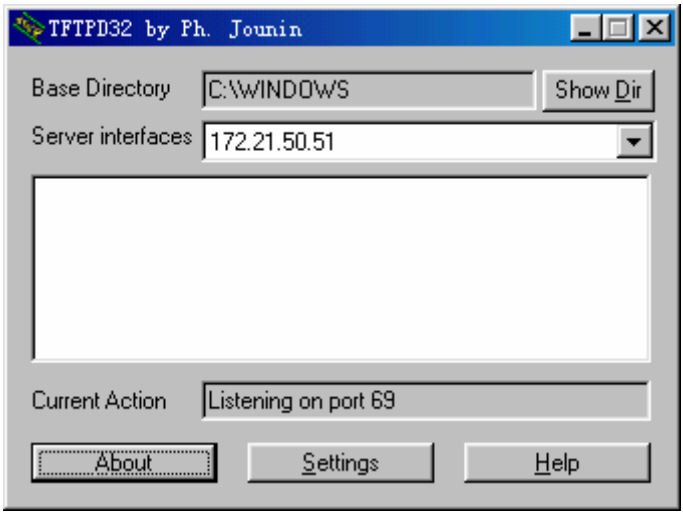


Figure 3-9 Interface of TFTP program

3) Click <Settings> to set the storage directory for the file to be loaded. In the "Base Directory" text box, input the storage directory "C:\IAD108V2R2" for the software to be loaded and other items take default values, as shown in Figure 3-10.

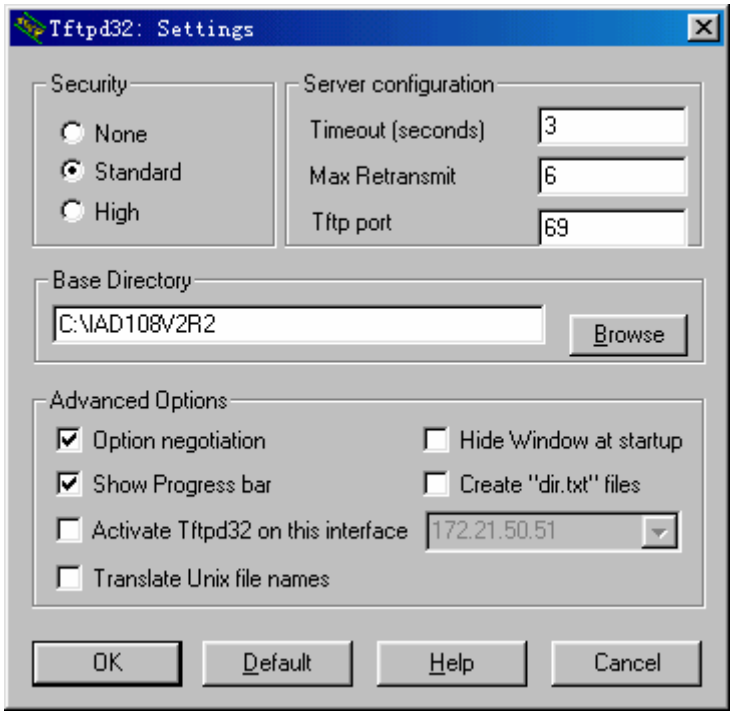


Figure 3-10 Set the storage directory for the software to be loaded

4) After select the directory of the files to be loaded, click <OK> to finish the settings of TFTP server.

3.2.2 Configuring FTP Server

When FTP is used to update IAD108 software, the new software is downloaded through network interface. To do this, a PC is used as the file server to run FTP server program.

Specific methods for configuring FTP server.

1) On IAD108, configure the user name and password for logging in to FTP server.

For instance, set the user name and password as "IAD" and "108".

```
IAD2000>enable
IAD2000#configure terminal
IAD2000(config)#ftpserver iad 108
{ <cr>|dirname<S><1,80> }:

Command:
                ftpserver iad 108
  Begin to save ftp server infomation, please wait a
minutes...
  ftp server login username : iad
  ftp server login password : 108
  ftp server directory name : .
IAD2000(config)#
```

2) Establish FTP server environment.

Configure the IP address of FTP server. Connect the FTP server and IAD108 through network interfaces. Make sure that the FTP server can ping IAD108.

3) Run the FTP server program.

Note:

In this manual, Serv-U is taken as an example to demonstrate how to configure FTP server on this PC. The installation program of FTP server is not delivered with the equipment, and you must get it by yourself.

Run the FTP program ”Serv-U” to enter the setting interface of FTP server as shown in Figure 3-11.

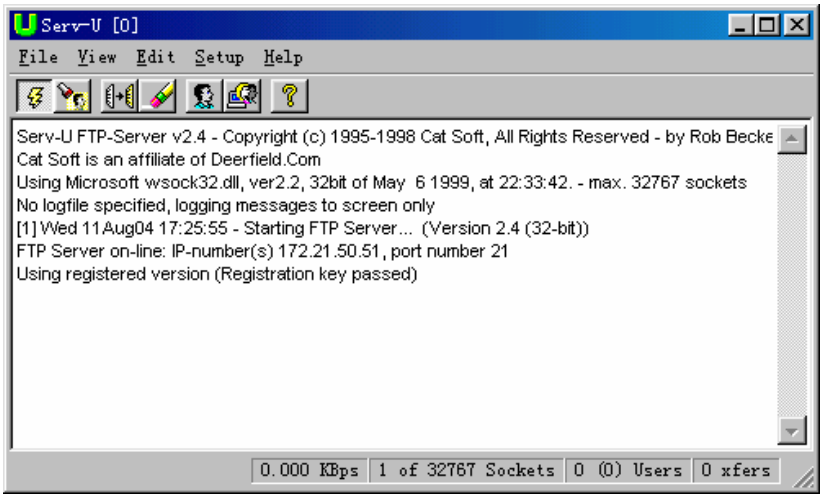

Serv-U [0]
File View Edit Setup Help
Serv-U FTP-Server v2.4 - Copyright (c) 1995-1998 Cat Soft, All Rights Reserved - by Rob Becke
Cat Soft is an affiliate of Deerfield.Com
Using Microsoft wsock32.dll, ver2.2, 32bit of May 6 1999, at 22:33:42. - max. 32767 sockets
No logfile specified, logging messages to screen only
[1] Wed 11Aug04 17:25:55 - Starting FTP Server... (Version 2.4 (32-bit))
FTP Server on-line: IP-number(s) 172.21.50.51, port number 21
Using registered version (Registration key passed)
0.000 KBps
1 of 32767 Sockets
0 (0) Users
0 xfers

Figure 3-11 Start interface of FTP program

4) Set login user name and password for Serv-U to log in to IAD108.

In the menu of Figure 3-11, select [Setup/Users…] to enter the user management interface and add a user.

Input the user name and password that have been preconfigured on IAD108. For example, set the user name as “IAD” and password as “108”. Then select the storage directory for the files to be loaded on this PC, as shown in Figure 3-12.

After confirming that all the above information is correct, click <Store> to save the newly added user.

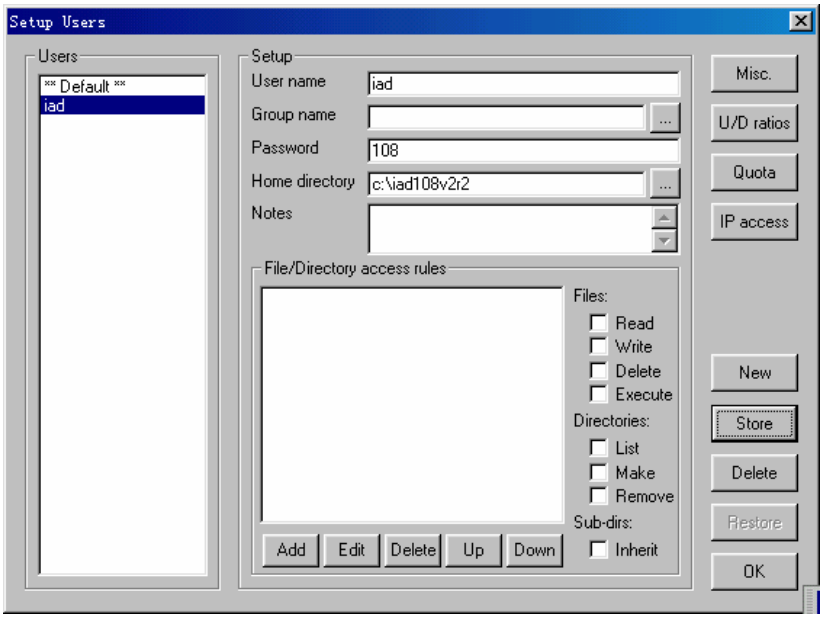


Figure 3-12 Add a new user

5) Set the authorities for accessing a file/directory

In the interface shown in Figure 3-12, click the <Add> below the “File/Directory access rules” text box to pop up the dialog box as

shown in Figure 3-13. Click <Browse> to select the storage directory for the files to be loaded, such as “C:\iad108v2r2”.

Then click <OK> to return to the interface as shown in Figure 3-14. At this time, the authority for accessing “C:\iad108v2r2” has been added into the “Path” text box.

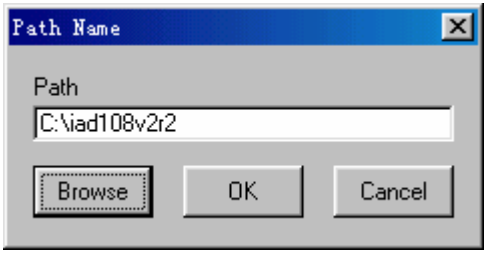


Figure 3-13 Select the directory of the files to be loaded

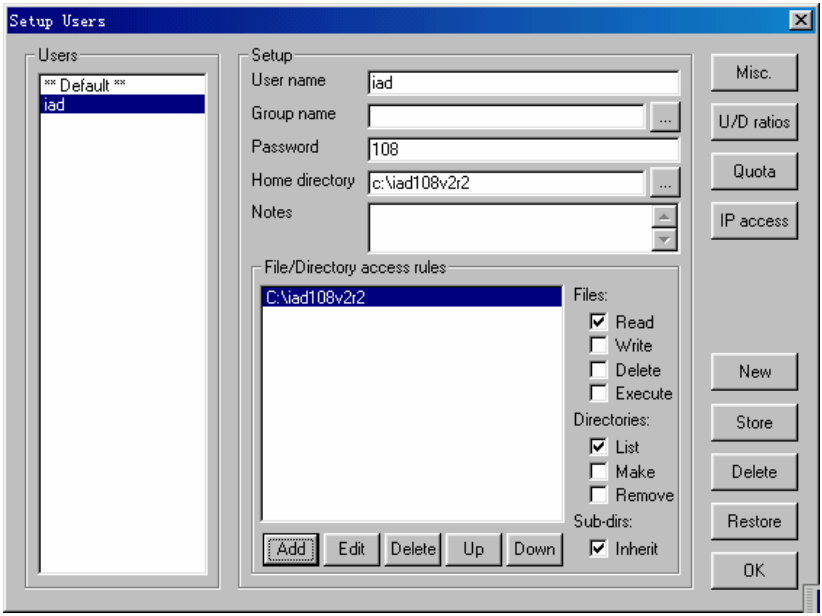


Figure 3-14 Set the authority for accessing a file/directory

Click the <OK> in the right lower corner of Figure 3-14 to finish the setting of Serv-U.

3.3 Loading Software

There are two modes for loading software: BIOS mode and host mode.

3.3.1 BIOS Mode

BIOS mode can only be used for local loading, and cannot be used for remote loading. The loading procedures are as follows.

1) Connect the serial ports of maintenance terminal and IAD108 through a serial port cable, and then turn on the HyperTerminal.
2) Reboot the system (through command **reboot**), and the following interface will be displayed.

```
IAD2000>enable
IAD2000#configure terminal
IAD2000(config)#reboot
  The config data has been changed, config will be lost
if reboot, continue? [Y|N]:y
  Are you sure to reset system? [Y|N]:y
  System will reboot in 5 seconds!
Press 't' to Test SDRAM :
Starting...

Init LAN switch ok.

**************************************************
*
                HUAWEI   IAD2000   SYSTEM   BOOT
          Copyright 2002-2005 Huawei Technology. Co.,
Ltd.
**************************************************
*
BIOS version:                    503
Creation date:                   Jun  8 2004, 16:38:15


auto-booting...
```

```
Attaching network interface lo0... done.

Attached TCP/IP interface to cpm0.
setting basic net para... done.

Please press CTRL+B to enter bootmenu,other key to boot!
remain  3s
```

3) In the above interface, press <Ctrl+B> within five seconds to enter the BIOS menu. If the boot program cannot find the applicable host program, DSP program and voice file in the Flash memory, it will enter BIOS interface automatically.

```
Welcome to bootmenu!

User name (<=20 chars):manager
User password (<=20 chars):
```

4) The system will prompt you to input user name and password. (Default user name and password are “manager” and “manager”). After inputting them, you can enter BIOS menu.

```
=======================
       BOOT MENU
=======================
 1.Enter equipment test
 2.Enter download submenu
 3.Show download zone information
 4.Boot system from flash
 5.Modify bootrom password
 R.Reset
```

```
Enter your choice(1-6 or R):
```

Items in the menu are listed in Table 3-1. Except 1 and 2, other items have no submenus.

Table 3-1 Meanings of the menu items in IAD108 BIOS

Menu	Meaning
1. Enter equipment test	Enter equipment test
2. Enter download submenu	Enter loading status
3. Show download zone information	Display the information of the file areas in the Flash memory
4. Boot system from flash	Start the system to enter the host program
5. Modify bootrom password	Modify the BIOS password
6. R.Reset	Reset the system

5) Select 2 to enter the following menu.

```
=======================
  FILE DOWNLOAD SUBMENU
=======================

 1. Enter serial submenu
 2. Enter ethernet submenu
 R. Return upper menu

 Enter your choice(1-2 or R):
```

Selecting “1”, you will enter serial port loading menu. Selecting “2”, you will enter network interface loading menu. Selecting “R”, you can return the upper level menu.

6) Select to load through serial port or network interface. In the following part, 1 and 2 are parallel, and you can only choose one to enter step 7.

- In the above menu, select “1” to enter serial port loading menu:

```
=======================
   SERIAL  SUBMENU
=======================

 1. Download file to Flash through serial interface
 2. Show serial parameter
 3. Set  serial parameter
 R. Return to file download submenu

 Enter your choice(1-3 or R):
```

Selecting 2 indicates to show the serial port parameter. Selecting 3 indicates to set the serial port parameter, (here only the baud rate can be modified). Selecting R means to return to the upper level menu.

- In the upper level menu, select 2 to enter the network interface loading submenu.

```
=======================
    FTP  SUBMENU
=======================

 1. Download file to Flash through ethernet interface
```

```
2. Show ethernet interface parameter
3. Modify  ethernet interface parameter
4. Show FTP download parameter
5. Modify FTP download parameter
R. Return to file download submenu

Enter your choice(1-5 or R):
```

Selecting 2 indicates to show the parameter settings of the network interface, such as the IP address. Selecting 3 means to modify the IP address and subnet mask. Selecting 4 indicates to show the FTP parameter setting (i.e., the IP address, password, user name and the file to be loaded of the FTP server. Selecting 5 means to modify the FTP parameter setting. Selecting R means to return to the upper level menu.

7) Selecting 1 to enter file loading selection menu.

```
=======================
  FILE SELECT SUBMENU
 =======================

  1. Download IAD program to flash
  2. Download local language file to flash
  3. Download gen language file to flash
  4. Download BIOS to flash
  5. Download VOICE file to flash
  6. Download DSP program to flash
  7. Download SLIC file to flash
  8. Download CPLD file to flash
  9. Download packet file to flash
  A. Download xDSL file to flash
```

```
R. Return to upper menu

Enter your choice(1-9 or R):
```

The meanings of the menu items are listed in Table 3-2.

Table 3-2 Meanings of BIOS file loading menu items

Item	Description
1. Download IAD program to flash	Load host program
2. Download local language file to flash	Load local language file
3. Download gen language file to flash	Load universal language file
4. Download BIOS file to flash	Load BIOS file
5. Download VOICE file to flash	Load voice file
6. Download DSP program to flash	Load DSP program
7. Download SLIC file to flash	Load SLIC file
8. Download CPLD file to flash	Load logic file
9. Download packet file to flash	Load file package
A. Download xDSL file to flash	Load xDSL file
R. Return to upper menu	Return to upper level menu

Note:

In the serial port loading selecting menu or the network interface loading selecting menu, if you select 1 you will enter the file loading selecting menu.

In the above menu, item 9 is very special: When BIOS selects 9 in the menu to load packet file, it will take all the files out of the packet (packet file consists of iad_voice and ida_dsp) to update the corresponding files in the Flash memory. So it is flexible. Loading and upgrading of a single file can be completed through other menu items.

8) Select the file and loading it.

According to the selection in step 6, the loading can be implemented through network interface and serial port. The following part describes these two modes.

- If you select network interface loading in step 6:

If the FTP server is correctly configured and the uplink interface of IAD108 can ping through FTP server, you can do it.

For the configuration of FTP server, refer to section 3.2.2 .

- If you select serial port loading in step 6:

When the above items are selected, you must transmit the corresponding files through the HyperTerminal within the default time allowed by the system.

Note:

- You can enter the “FILE SELECT SUBMENU” menu by clicking “SERIAL SUBMENU”/”1. Download file to Flash through serial interface”, or “FTP SUBMENU”/”1. Download file to Flash through Ethernet interface”.
- The operations made after you entering “FILE SELECT SUBMENU” through “SERIAL SUBMENU” is different from those after entering through "FTP SUBMENU”. If you enter through “SERIAL SUBMENU”, you need to perform file transmission. If you enter through “FTP SUBMENU”, you can directly load the file to the Flash memory.

After entering the “FILE SELECT SUBMENU” menu through “SERIAL SUBMENU”/”1. Download file to Flash through serial interface”, select load file “9”. The interface is displayed as follows:

```
=======================
  FILE SELECT SUBMENU
=======================

  1. Download IAD program to flash
  2. Download local language file to flash
  3. Download gen language file to flash
  4. Download BIOS to flash
  5. Download VOICE file to flash
  6. Download DSP program to flash
  7. Download SLIC file to flash
  8. Download CPLD file to flash
  9. Download packet file to flash
  A. Download xDSL file to flash
```

```
  R. Return to upper menu


  Enter your choice(1-9 or R):9
  ============================================
  Down load file by xmodem_crc protocol....  CCCCCC
```

When the above prompt appears on the terminal, select [Transfer/Send File] in the HyperTerminal window, then select the file to be loaded, set the transmission protocol as Xmodem, and click <Send>.

When IAD108 and HyperTerminal are correctly connected, and the file transmission starts, the transmission progress will be shown on HyperTerminal.

When the loading succeeds, the following prompt will appear and the system will return to the menu interface of selecting loading file.

```
  Down load file by xmodem_crc protocol end
  ========================================
Download file successful.
Check file CRC value... done.

Copy file (voice resource) to flash(0x10300000),please
wait...... Done.
Save file end.
The file of you download check successful, and copy to
flash ok!

 ======================
  FILE SELECT SUBMENU
```

```
=======================

 1. Download IAD program to flash
 2. Download local language file to flash
 3. Download gen language file to flash
 4. Download BIOS to flash
 5. Download VOICE file to flash
 6. Download DSP program to flash
 7. Download SLIC file to flash
 8. Download CPLD file to flash
 9. Download packet file to flash
 A. Download xDSL file to flash
 R. Return to upper menu

 Enter your choice(1-9 or R):
```

If you select to go on loading other files, the above loading process will be repeated.

9) When all the files have been loaded, you need to select “R” in the submenus to return to the BootMenu. In the main menu, you can select Reset to restart the system to enter the interface of main program.

Note:

- When the serial port loading is implemented, the system will be restarted. The rate of serial port will be automatically restored to 9600 bit/s. If the HyperTerminal does not display normally, you should adjust the attributes of the HyperTerminal and change the baud rate to 9600 bit/s.
- When loading through serial port, generally the transmission rate is slow. You can accelerate the loading rate through command line, and the highest rate is 115200 bit/s.

3.3.2 Command Line Loading Mode

IAD108 can also be loaded in command line mode. In this mode, you can only load the package file iad_packet. It contains the four files needed for upgrading IAD108: iad_voice, iad_dsp, iad_prog.lzw, and iad_bios. Based on different transmission modes, there are three modes: Xmodem protocol mode, FTP mode, and TFTP mode.

When Xmodem protocol mode is used, you can only transmit files through serial port. This mode is suitable for local loading. However, its transmission speed is very low. In FTP/TFTP mode, the network interface is used to transmit the files. It is used in both remote loading and local loading. In remote loading, as FTP is more reliable than TFTP, FTP is recommended.

I. Loading File Through Xmodem Protocol

1) Connect the serial ports of maintenance terminal and IAD108 through a serial port cable, and establish the HyperTerminal connection.
2) On the HyperTerminal, enter command **load** and press <Enter>.

Example: Load package file through Xmodem protocol.

```
IAD2000#load system dsp xmodem
IAD2000(config)#load packet xmodem
  Load(backup) begins. This process will take several
minutes. If it is  interrupted unproperly, it will fail.
Please wait and check the result.
  Besides, you can use command 'show progress load' to
display the progress  information.

  Please select "Send file"sub menu of "Send" main menu
to send file...
CCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCCC
```

3) Select [Transfer/Send File] on HyperTerminal. The protocol type should be "Xmodem". After select the files to be sent, click <Send>. After the loading begins, the transmission progress will be shown on the terminal.

Note:

- When loading files through the serial port by using Xmodem protocol, it takes a long time. Please wait patiently, and do not reboot the system.
- To speed up the loading speed, you can use command **baudrate** to set the communication rate to 115200 bit/s, and set the communication rate of console to 115200 bit/s too. Otherwise, the communication will fail.
- During the rebooting of the system after the loading is finished, the serial port speed will be automatically recovered to 9600 bit/s.

4) After the files are completely sent, the following information will be displayed.

```
IAD2000#
  OPERATION TYPE:    Load operation
  FILE TYPE:         Packet file
  OPERATION STAGE:   save file
  PROCESS:           92%

  OPERATION TYPE:    Load operation
  FILE TYPE:         Packet file
  OPERATION RESULT:  Operation complete
  FAILURE REASON:    Vacancy

IAD2000#
```

5) If you need to load other files, repeat steps 2 and 3. The loaded file can only take effect after the system is rebooted. To reboot the system, you can execute the command reboot in privilege mode.

Example: In privilege mode, input command **reboot** to reboot the system.

```
IAD2000#reboot
  The config data has been changed, config will be lost
if reboot, continue? [Y|N]:y
  Are you sure to reset system? [Y|N]:y
  System will reboot in 5 seconds!
```

II. Loading File Through TFTP/FTP

1) In local loading, connect the serial ports of the maintenance terminal and IAD108 through a serial port cable, and then turn on the HyperTerminal. In remote loading, use Telnet program to log in to the device.
2) Connect the IAD108 with the FTP server/TFTP server through a network cable. Make sure that the server can ping the IAD108. For the settings of FTP server/TFTP server, refer to section 3.2.1. The IP address of the IAD108 can be check through command **show ip address**, or be modified through command **ip address**.
3) Run the FTP program or TFTP program on the file server.
4) To start the FTP server program, you need to set the following items on the maintenance terminal: user name and password used to log in to the FTP server, and path of the file to be loaded. If you use TFTP to load, the latter operation is unnecessary.

```
IAD2000(config)#ftpserver iad 108
C:\WINDOWS\Desktop\IAD108V2R2
  Begin to save ftp server infomation, please wait a
minutes...
```

```
  ftp server login username : iad
  ftp server login password : 108
  ftp server directory name :
C:\WINDOWS\Desktop\IAD108V2R2
```

Note:

- In the above command, "IAD108" is a legal user name in the FTP server, the password is "passwd", and the path of the file to be loaded is "C:\IAD108 B01D030". Such settings must be consistent with those set in FTP Serv-U.
- To use FTP for loading, first execute command **ftpserver**. After that, carry out command **write** to save the configurations in command **ftpserver** to the device. After that, when the device is loaded through FTP in next rebooting, the command **ftpserver** needs not be carried out.
- Format of command **ftpserver**: **ftpserver** *username password* [*dirname*]. In this command, *username* and *password* are the name and password used to log in to the FTP server, and *dirname* is the directory name of FTP server. This command is used in global config mode.

---

5) On the maintenance terminal, enter command **load packet** to load the package file. During the loading, you can use command **show progress load** to check the loading progress.

```
IAD2000(config)#load packet ftp 172.21.50.51 iad_packet
  Load(backup) begins. This process will take several
minutes. If it is interrupted unproperly, it will fail.
Please wait and check the result.
  Besides, you can use command 'show progress load' to
```

```
display the progress  information.

IAD2000(config)#
  OPERATION TYPE:    Load operation
  FILE TYPE:         Packet file
  OPERATION STAGE:   file is transmitted into board from
outside
  PROCESS:           10%

  OPERATION TYPE:    Load operation
  FILE TYPE:         Packet file
  OPERATION STAGE:   file is transmitted into board from
outside
  PROCESS:           85%

  OPERATION TYPE:    Load operation
  FILE TYPE:         Packet file
  OPERATION STAGE:   save file
  PROCESS:           1%

  OPERATION TYPE:    Load operation
  FILE TYPE:         Packet file
  OPERATION STAGE:   save file
  PROCESS:           80%

  OPERATION TYPE:    Load operation
  FILE TYPE:         Packet file
  OPERATION RESULT:  Operation complete
  FAILURE REASON:    Vacancy
```

```
IAD2000(config)#
```

6) To load other files, repeat step 4. After all the programs loaded, use command **reboot** to reset the system and make the new programs valid. Before rebooting, make sure that the formerly configured data has been saved through command **write**.

Chapter 4 Configuring Data

In this chapter, the methods and steps for configuring IAD108 data through command line are introduced.

4.1 Preparations Before Configuration

Before configuring IAD108, you should prepare the basic data of this IAD108 and know the user name and password used for logging into the device.

4.1.1 Collecting Data

Before configuring data, you must plan the data of IAD108, such as IP address of IAD108, and IP address of the related servers. Since IAD108 interworks with Media Gateway Controller (MGC), you should also plan the data for the interconnection between them.

The IP addresses need to be planned are listed in Table 4-1.

Table 4-1 IP address allocation table

No.	Item	Remarks
1	IP address of IAD108	None.
2	IP address of the default gateway for IAD108's uplink	LAN Switch or low end router
3	IP address of MGC	In this manual, SoftSwitch is taken as an example of MGC.

No.	Item	Remarks
4	IP address of Loghost	Loghost is the host used for generating and storing logs.
5	IP address of Network Management Station (NMS)	NMS is the network management station that runs IAD Management System (IADMS).
6	IP address of Domain Name server (DNS)	DNS is the Domain Name server.
7	IP address of Simple Network Time Protocol (SNTP) server	”SNTP” indicates the Simple Network Time Protocol server.

Note:

In the above table, the IP addresses of NMS, DNS, SNTP, and Loghost are not mandatory. If IAD108 is not configured with the server, the corresponding IP address will be unnecessary.

Table 4-2 Parameters for interconnection with MGC

Data need to be configured on MGC	Data need to be configured on IAD108
IP address of IAD108	IP address of MGC
Port number of User Datagram Protocol (UDP)	Port number of transfer layer protocol
Type of control protocol	Type of control protocol

Data need to be configured on MGC	Data need to be configured on IAD108
Encoding type	Encoding type
Type of transfer protocol	Type of transfer protocol
Domain name of IAD108	Domain name of IAD108
Interface name of IAD108	Interface name of IAD108 (local name)
Domain name of MGC	Domain name of MGC

4.1.2 Login Environment

After the system is loaded and rebooted, the following interface will appear.

```
IAD2000#reboot
  The config data has been changed, config will be lost
if reboot, continue? [Y|N]:y
  Are you sure to reset system? [Y|N]:y

  System will reboot in 5 seconds!
Press 't' to Test SDRAM :
Starting...

Init LAN switch ok.

**************************************************
******************
                HUAWEI   IAD2000   SYSTEM   BOOT
          Copyright 2002-2005 Huawei Technology. Co.,
```

```
Ltd.
*****************************************************
******************
BIOS version:                    506
Creation date:                   Jul 12 2004, 10:16:22


auto-booting...

Attaching network interface lo0... done.

Attached TCP/IP interface to cpm0.
setting basic net para... done.

Please press CTRL+B to enter bootmenu,other key to boot!
remain  0s
```

According to the prompt, you can press any key to go to the next step, or wait for 5 seconds and the system will automatically enter the next step. You can press <CTRL+B> to enter the BIOS interface to operate. Refer to section 3.2.1 in Chapter 3.

```
Begin to check program area in flash... done..
Copy program from area(1) to ram!
Expand                     file                     to
ram  ..................................
.....................................................
.
.....................................................
.
.....................................................
```

```
.
.....................................................
.
.....................................................
.
.....................................................
.

Starting at 0x10000...

Init LAN switch ok.Attached TCP/IP interface to cpm unit
0
Attaching network interface lo0... done.
NFS client support not included.

setting basic net para... done.
No record in exception buffer!

Initialize and check system config data... done.

Start Initialize SPI.
DSP Initialize Succeed .

SPI module initialized OK.
MIB initialization OK!

 wait agent ...
Begin            Register            to            IADMS
1 ........................................
```

```
 Time out when registering to IADMS 1
Searching modification on system config data while
initializing...
Nothing modified.
```

When the device has been started successfully, the following interface will pop up to prompt you to input user name and password. By default, IAD108 has a super manager, whose user name is “root” and password is “admin”. Note that the password is case sensitive, while the user name is not. Here, take the super manager as an example, enter the user name “root” and password “admin” (it is not displayed on the screen). The following prompt will appear.

```
User name (<=15 chars):root
User password (<=15 chars):
IAD2000>
```

When the prompt “IAD2000>” appears on the screen, it means that you have logged into the system successfully.

After logging into the system for the first time, you must modify the login password of the super manager. The command **user password** in privilege mode is used to modify the password. Note that the password is case-sensitive and the maximum length is 15 characters.

Caution:

If the super manager “root” forgets the password, contact the technical support engineer of Huawei.

Example: Enter global config mode to modify the password of user “root“.

```
IAD2000>enable
IAD2000#configure terminal
IAD2000(config)#user password
  User Name(<=15 chars):root
  Old Password(<=15 chars):
  New Password(<=15 chars):
  Confirm Password(<=15 chars):
  Changed ok!
  Continue? [Y|N]:n
IAD2000(config)#
```

When the system prompts “Continue? [Y|N]”, if you want to modify the passwords of other users, you can input “Y” to go on. Otherwise, you can input “N” and press <Enter>. The system default value is “N”.

Note:

For the commands related to the management of users, you can refer to Section 5.1.3 of Chapter 5.

4.2 Basic Commands

A command prompt of IAD108 consists of two parts: fixed character string + command mode identifier. The command mode identifier indicates the mode in which the current command is in. For

example: “>” indicates that the command mode is user mode, while # indicates privilege mode. In the global config mode, you can use the command **hostname** to configure the fixed character string. By default, the fixed character string of the system is “IAD2000”.

Example: Modify the default host name of the system into “IAD108”.

```
IAD2000(config)#hostname IAD108
  To change command line prompt is ok
IAD108(config)#
```

This command is executed successfully, and the host name has been changed into “IAD108”.

4.2.1 Command Modes

IAD108 has the following command modes: User mode, privilege mode, global config mode, advanced mode, debug mode, and LAN switch mode. During data configuration, commands are frequently used to switch over the command modes and save the data.

Note:

It is unusual to use the commands in advance mode and debug mode to configure and maintain the device, therefore, only the features and usage of some usually used commands are introduced in this manual.

The commands used in advance mode and debug mode can be found in Appendix A.

The privilege mode and global config mode are compatible with the lower-authority modes.

- In the privilege mode, you can run the commands in the user mode.
- In the global config mode, you can run all the commands in the user mode and privilege mode.

The relations among the command modes are shown in Figure 4-1. The oval circles in the figure represent different command modes, each arrow indicates the change from one mode to another mode. The mode change commands are appended to the arrows.

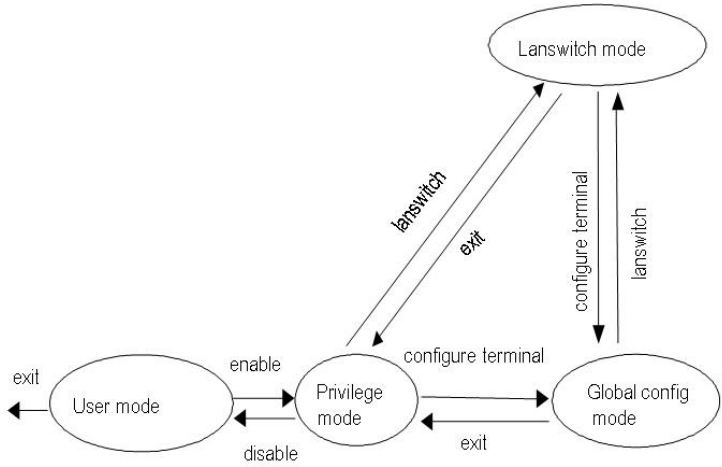


Figure 4-1 Relations among different command modes

Example: To switch from privilege mode to global config mode, carry out command **configure terminal**. To exit from global config mode to privilege mode, carry oute command **exit**.

4.2.2 Usually Use Commands

The usually used commands and their functions are listed in Table 4-3.

Table 4-3 List of usually used commands

Command	Function
IAD2000>**enable**	Enter the privilege mode
IAD2000#**configure terminal** IAD2000(lanswitch)# **configure terminal**	Enter the global config mode
IAD2000# **lanswitch** IAD2000(config)#**lanswitch**	Enter the LAN Switch mode
Disable (any mode)	Exit from current mode and enter the user mode
Exit (any mode)	Exit from current mode and enter the previous mode, or exit from the configuration environment
language (any mode)	Modify current language mode
Write (any mode)	Save data immediately
IAD2000>**cls**	Clear the screen
IAD2000>**show version**	Show the version of the equipment
IAD2000(config)#**user password**	Modify user name and password

Caution:

To prevent data loss caused by system rebooting or power-off, you can execute command **write** in privilege mode to save the configured data.

4.2.3 Examples

I. Entering Global Config Mode from Privilege Mode:

```
IAD2000#configure terminal
IAD2000(config)#
```

II. Modifying Current Language Mode

```
IAD2000(config)#language
  The current language mode has been switched.
IAD2000(config)#
```

III. Saving Data

```
IAD2000(config)#write
  Command executing, please wait...
System starts to save configuration data, please wait a
moment......
The configuration data backup percent is: 100%
IAD2000(config)#
```

IV. Showing Version of Equipment

```
IAD2000#show version
```

```
  Equipment type            : IAD108
  Main Board PCB version    : AG21CSPA VER.A
  Software version          : IAD2000V200R002B01D031
  BIOS version              : 506
  SLIC version              : (U35-U38)015
  CPLD version              : (U16)100
  DSP version               : (U34)V100R1C1B23D10
IAD2000#
```

4.3 Process of Data Configuration

The configuration of basic data is the basis for other configurations. Only when the correctness and validity checks of the basic data have been implemented, can you configure interface data, access user data, protocol data and software parameters.

Table 4-4 shows the configuration procedures.

Table 4-4 Data configuration process of IAD108

Steps	Operation
Step 1	Configure basic data of the equipment
Step 2	Configure voice user data
Step 3	Configure MG attribute data
Step 4	Configure protocol data (optional)
Step 5	Configure software parameter (optional)

After you have finished the configuration of a group of data, you can run the command **show running-config** in privilege mode to

check the correctness of the configured data. If you want to check the initial configuration of the system, you can execute command **show startup-config** in the privilege mode.

Note:

- Except that the first step is mandatory, other steps are parallel without strict sequence.
- Steps 4 and 5 are optional because the system has default values.

4.4 Configuring Basic Data of the Equipment

Configuration of equipment basic data include: Information of this device, IP address, time, and the configurations of all the related servers. The IP address is most important and must be configured, while other data can be configured optionally according to the actual conditions.

Although there is no strict requirement on sequence, it is recommended to configure the data according to the sequence listed in Table 4-5.

4.4.1 Task List

Note:

The configuration tasks are arranged from the very beginning of your configuration procedures.

Table 4-5 Task list of configuring equipment data

Serial No.	Operation	Command
1	Configure data of this device	**banner incoming** *hostname phone*
2	Configure IP address of IAD108 (mandatory)	Configure fixed IP address: **ip address** *ip-address net-mask gateway-ip*
		Configure the system to obtain IP address automatically: **dhcp enable**
		Configure PPPoE to obtain IP address automatically: **pppoe username** *usermane* **password** *password* **pppoe** { **disable** | **enable** }
3	Set the system time of IAD108	Set the system time of IAD108 to be synchronous with SNTP server: **sntp server** {**address** *server-ip* | **name** *server-name*} **sntp time-zone** *sign value* **sntp interval** interval-seconds

Serial No.	Operation	Command
		Set system time of IAD108: **clock set** *hh:mm:ss yyyy-mm-dd*
4	Configure the domain name and IP address of DNS	**dns domain-name** *name* **dns server** *first* { *second* | *third* }
5	Add an NMS	Configuring device ID: **eid** *eid*
		Configure IADMS information: **iadms** *adms-num nmsaddress getcommunity setcommunity trapcommunity* [*nmsTrapPort*]

4.4.2 Configuring the Data of This Equipment

When you log in to the IAD108 from the serial port or from a Telnet connection, you will see some welcome messages, including the name of the device, and the contact telephone number. You can set or change these messages with the command **banner incoming** *hostname phone* in global config mode.

Note:

hostname is used to identify the device in the network and can be configured randomly.

In usual cases, it is configured according to the customer's requirements. If there is no requirements, it is recommended to name it in the following format:

Hostname = office name + MG type

*office name = country + city + location + operator name

Example: Configure an IAD for Huawei:

- *Hostname*: SZ-BT-HW-IAD108
- *phone*: 0755-12345678.

```
IAD2000#configure terminal
IAD2000(config)#banner incoming
  Please input location name(<20 chars): SZ-BT-HW-IAD108
  Please input phone number(example:010-88888888):
0755-12345678
  Hostname config success
IAD2000(config)#write
  Command executing, please wait...
System starts to save configuration data, please wait a
moment......
The configuration data backup percent is: 100%
```

After configuration, log in the device again. The information of this office configured just now will be shown in the prompt.

```
IAD2000(config)#reboot
  Are you sure to reset system? [Y|N]:y
```

```
  System will reboot in 5 seconds!
Press 't' to Test SDRAM :
Starting...

Init LAN switch ok.

*******************************************************
*
                HUAWEI   IAD2000   SYSTEM   BOOT
          Copyright 2002-2005 Huawei Technology. Co.,
Ltd.
*******************************************************
*
BIOS version:                   506
Creation date:                  Jul 12 2004, 10:16:22


auto-booting...

Attaching network interface lo0... done.

Attached TCP/IP interface to cpm0.
setting basic net para... done.

Please press CTRL+B to enter bootmenu,other key to boot!
remain  0s
Begin to check program area in flash... done..
Copy program from area(1) to ram!
Expand                      file                      to
```

```
ram  ..................................
.....................................................
.
.....................................................
.
.....................................................
.
.....................................................
.
.....................................................
.
.....................................................
.

Starting at 0x10000...

Init LAN switch ok.Attached TCP/IP interface to cpm unit
0
Attaching network interface lo0... done.
NFS client support not included.

setting basic net para... done.
No record in exception buffer!

Initialize and check system config data... done.

Start Initialize SPI.
DSP Initialize Succeed .
```

```
SPI module initialized OK.
MIB initialization OK!

Searching modification on system config data while
initializing...
Nothing modified.
      ****************************************
      *                                      *
      *    IAD2000  Integrated Access Device   *
      *                                      *
      ****************************************
    Copyright 2002-2005 Huawei Technology. Co., Ltd.
                Location Name: SZ-BT-HW-IAD108
                Phone  Number: 0755-12345678
```

4.4.3 Configuring IP Address of IAD108

IP address is an important parameter of IAD108, and it must be configured. After being configured, the IP address can take effect immediately without rebooting. The IP address of IAD108 can be got in three ways:

- Configure fixed IP address
- Dynamically obtained from the DHCP server
- Obtained through PPPoE dialup mode

You can use the command **show ip address** in user mode to check the IP address of IAD108.

```
IAD2000>show ip address
-------------------------------------------------
  ip address     : 172.21.100.16
```

```
  subnetwork mask: 255.255.0.0
  default gateway: 172.21.200.250
  MAC address    : 00-E0-FC-1E-24-88
  PPPoE disable
  vlan tag function is disable
  vlan id        : 0
  vlan priority  : 3
  DHCP function is disable
  TOS of voice packets:  Maxmize reliability
  TOS of other packets:  Normal service
--------------------------------------------------
IAD2000>
```

I. Configuring Fixed IP Address for IAD108

In global config mode, you can use the following command to configure the fixed IP address for IAD108.

ip address *ip-address net-mask gateway-ip*

ip-address, *net-mask*: IP address and subnet mask of IAD108.

Example: Configure the fixed IP address of IAD108 as “172.21.100.16”, and subnet mask as “255.255.0.0”, while default gateway as “172.21.200.250”.

```
IAD2000(config)#ip address 172.21.100.16 255.255.0.0
172.21.200.250
  Changing net parameter may affect current service,
continue?[Y|N]:y
  Command executing, please wait...
--------------------------------------------------
```

```
  ip address     : 172.21.100.16
  subnetwork mask: 255.255.0.0
  default gateway: 172.21.200.250
-------------------------------------------------
IAD2000(config)#
```

II. Configuring IAD108 to Obtain IP Address Through DHCP

To dynamically obtain the IP address, IAD108 needs to cooperate with DHCP server, and the DHCP server in the network must work and communicate with IAD108 normally.

When configuring data for IAD108, you can execute command **dhcp enable** to start the DHCP client. The commands are listed in Table 4-6.

Table 4-6 Commands used to obtain IP address dynamically

Operation	Command
Prohibit DHCP	IAD2000(config)#**dhcp disable**
Refresh IP address	IAD2000(config)#**dhcp renew**

Example: Configure IAD108 to dynamically obtain the IP address through DHCP.

1) Check the current configuration of IAD108 before configuring it.

```
IAD2000(config)#show ip address
-------------------------------------------------
  ip address     : 172.21.100.16
  subnetwork mask: 255.255.0.0
```

```
  default gateway: 172.21.200.250
  MAC address    : 00-E0-FC-1E-24-88
  PPPoE disable
  vlan tag function is disable
  vlan id        : 0
  vlan priority  : 3
  DHCP function is disable
  TOS of voice packets:  Maxmize reliability
  TOS of other packets:  Normal service
-------------------------------------------------
IAD2000(config)#
```

2) The result shows that the DHCP function is prohibited currently. Start the DHCP function.

```
IAD2000(config)#dhcp enable
  Changing net parameter may affect current service,
continue?[Y|N]:y
  Command executing, please wait...
-------------------------------------------------
  ip address     : 172.21.50.79
  subnetwork mask: 255.255.0.0
  default gateway: 172.21.200.250
-------------------------------------------------
IAD2000(config)#
```

3) The command has been executed successfully, and check the IP address again.

```
IAD2000(config)#show ip address
-------------------------------------------------
  ip address     : 172.21.50.79
  subnetwork mask: 255.255.0.0
```

```
  default gateway: 172.21.200.250
  MAC address    : 00-E0-FC-1E-24-88
  PPPoE disable
  vlan tag function is disable
  vlan id        : 0
  vlan priority  : 3
  DHCP function is enable
  TOS of voice packets:  Maxmize reliability
  TOS of other packets:  Normal service
-------------------------------------------------
IAD2000(config)#
```

4) The result shows that the DHCP function has been started, and the IP address “172.21.50.79” is obtained from the DHCP server.

III. Configuring IAD108 to Obtain IP Address Through PPPoE Dialup

IAD108 supports PPPoE dialup mode. It can obtain IP address from the DNS server during the PPPoE dialup process and perform DNS resolution.

Configuration for PPPoE can be made in two steps:

1) Configure user name and password
2) Enable PPPoE

If PPPoE dialup fails, the system will automatically dial up again. The commands are listed in Table 4-8.

Table 4-7 Commands for IAD108 to obtain IP address through PPPoE dialup

Operation	Command
Configure PPPoE user name and password	IAD2000(config)#**pppoe username** *usermane* **password** *password*
Enable PPPoE	IAD2000(config)#**pppoe** { **disable** | **enable** }
Show PPPoE configuration	IAD2000>show pppoe

username: PPPoE user name, a character string ranging 1–31 characters.

password: PPPoE user password, a character string ranging 1–31 characters.

The user name and password are used on the broadband access server (BAS) for authenticating the user. They must be consistent with those configured on the BAS.

Example: Configure IAD108 to obtain IP address through PPPoE dialup mode. The operations are as follows.

3) Set the PPPoE user name as “zw@isp”, and password as “huawei”.

```
IAD2000(config)#pppoe username zw@isp password huawei
IAD2000(config)#
```

4) Start PPPoE function

```
IAD2000(config)#pppoe enable
IAD2000(config)#
```

5) Check PPPoE configurations

```
IAD2000(config)#show pppoe
-------------------------------------------------
```

```
  PPPoE offline
  PPPoE user name: zw@isp
  PPPoE password : huawei
-------------------------------------------------
IAD2000(config)#
```

Caution:

Because a correct IP address is the basis for the IAD108 to communicate with other devices, do not randomly change the IP address when the IAD108 is working normally.

4.4.4 Configuring System Time of IAD108

IAD108 needs correct time for functions like local accounting, alarm report, call tracing and log output. Therefore, precise system time should be configured.

You can configure the system time of IAD108 by yourself, or configure it to synchronize with SNTP server. If SNTP is turned on, the system time be obtained from SNTP server with preference and periodically synchronized. In this way, you can ensure that the time of IAD108 is the same as that of other devices controlled by the same SNTP server.

I. Configuring System Time for This Device

You can use the command **clock set** *hh:mm:ss yyyy-mm-dd* in global config mode to set the system time for this device. Before setting the system time, you can use the command **show clock** in user mode to check whether the system time is correct.

Example:

Show the system time.

```
IAD2000>show clock
-------------------------------------------------
  System startup date: 2004-08-12 time: 11:01:59
  Current date: 2004-08-12
  Current time: 11:54:16
-------------------------------------------------
IAD2000>
```

Modify the system time to 2003-07-11, 15:30:01.

```
IAD2000(config)#clock set 12:10:10 2004-08-12
  Current date: 2004-08-12
  Current time: 12:10:10
IAD2000(config)#
```

II. Starting SNTP Client

To start the SNTP client on IAD108, you need to execute the following three commands:

- **sntp server** {**address** *server-ip* | **name** *server-name*}
- **sntp time-zone** *sign value*
- **sntp interval** *interval-seconds*

After the SNTP client is configured, you can use the command **show sntp status** in privilege mode to check it.

Example: Start SNTP client on the IAD108, specifying the name of the SNTP server as “SNTP-SVR”, time zone as East 8, and synchronization interval as 60 seconds.

```
IAD2000(config)#sntp server name sntp-svr.tele.com
IAD2000(config)#sntp time-zone + 8
IAD2000(config)#sntp interval 60
IAD2000(config)#show sntp status
-----------------------------------------------------
-
NTP server:      sntp-svr.tele.com
Local time zone : +8
Synchronization interval : 60Sec.
-----------------------------------------------------
-
IAD2000(config)#
```

Caution:

- If you want to specify the SNTP server with the name “sntp-svr.tele.com”, you should first start DNS client on the IAD108, then configure the SNTP client. Otherwise, you can only use the IP address 210.11.123.5 to access the SNTP server.
- After you have started SNTP client on the IAD108, the start and end time of the log information and accounting information will all subject to the time provided by the SNTP server. In this case, the local time on the IAD108 that is configured with the command **clock set** will not take effect.

4.4.5 Starting DNS Client

After the DNS client is started on IAD108, IAD108 can access other network devices through domain name other than only through the IP address. The data of DNS client is not mandatory.

In global config mode, you can use the following two commands to configure the DNS client of IAD108.

- **dns domain-name** *name*
- **dns server** *first* { *second* | *third* }

After configuration, you can use the command **show dns status** in privilege mode to check the status of DNS. To delete the configurations, use the following commands in global config mode:

- **no dns domain-name** *name*
- **no dns server** *first* { *second* | *third* }

Example: After starting the DNS client on IAD108, configure the domain name of the DNS domain as “tele.com” and the IP address of DNS server as “210.11.123.13”.

```
IAD2000(config)#dns domain-name tele.com
IAD2000(config)#dns server 210.11.123.13
{ <cr>|second<I> }:

Command:
                dns server 210.11.123.13
IAD2000(config)#show dns status
------------------------------------------------------
-
Domain name:tele.com
Server address:
210.11.123.13
------------------------------------------------------
-
IAD2000(config)#
```

4.4.6 Adding IADMS

In NGN, many IADs are running, and it is very difficult for one NMS to manage all of them. So a hierarchical management mode is used, in which a certain number of IADs are managed directly by an IADMS, and multiple IADMSs are managed by the iManager N2000 NMS. An IADMS is a software system running on a workstation.

To configure an IAD108 as be managed by an IADMS, you must configure equipment ID (EID) for the IAD108. The EID must be consistent with that configured on the IADMS, because IADMS

identifies the IAD108 by this ID. After that, you can add other information for this IADMS.

I. Command modes

In global config mode, you can use the following commands to configure the equipment ID and add an IADMS.

- **eid** *Equipment-ID*
- **iadms** *iadms-num ip getcommunity setcommunity trapcommunity* [*nmsTrapPort*]

II. Descriptions of parameters

Table 4-8 Parameters of the commands used to add an IADMS

Item	Description
Equipment-ID	Unique ID of the IAD used in IADMS, it is character string ranging 1–32 characters.
iad ms-num	Number of IADMS, ranging 0–1.
ip	IP address of IADMS
getcommunity/ setcommunity	Names of the GET/SET communities of the IADMS. The GET/SET community names can be any character string less than 15 characters. A community name is a simple security guarantee mechanism provided by Simple Network Management Protocol (SNMP), which is similar to user password. The IAD108 shall decide whether to accept an NM request by comparing the GET/SET community name configured on itself and that configured on the IADMS. By default, the GET community name is “public” and the “SET” community name is “private”, and you can change the community names by yourself.
nmsTrapPort	Trap port number used by the IADMS, which is 162 by default.

III. Usage example

Example:

Set the equipment EID of IAD108 as “cn108.com”.

```
IAD2000(config)#eid cn108.com
IAD2000(config)#
```

Add an IADMS with the IP address as 210.11.123.33:

```
IAD2000(config)#iadms 1 ip 210.11.123.33 get set trap 162
IAD2000(config)#
Register to IADMS while booting
```

Table 4-9 Other related command

Operation	Command
Set whether the IAD registers to IADMS when it starts.	IAD2000(config)#**iadms** *iadms-num* **register** { *enable* | *disable* }
Display the IADMS information.	IAD2000>**show iadms**
Delete the IADMS configuration.	IAD2000>**show iadms**

To set the IAD108 to register to IADMS at startup, operate as follows:

```
IAD2000(config)#iadms 1 register enable
IAD2000(config)#
```

To query the IADMS configuration information, operate as follows:

```
IAD2000(config)#show iadms
```

```
IADMS0:
 not configured
IADMS1:
 IADMS address              : 210.11.123.33
 IADMS host name            :
 Use IADMS name to register : No
 Get community              : get
 Set community              : set
 Trap community             : trap
 Trap port                  : 162
 Register to IADMS while booting
-------------------------------------------------
 Handshake interval  : 30sec
 Handshake switch    : on
-------------------------------------------------
 Register state      : failed
IAD2000(config)#
```

Note:

- When adding an IADMS, you must ensure that the IP address of the IADMS is unique.
- Command **iadms** can either be used to add an IADMS, or modify an IADMS.
- The character string of a community name is case-sensitive, which means the same character strings with different cases will be regarded as different community names.
- After the IADMS is configured, you need to activate it by using command **iadms** *iadms-num* **register enable**.

4.5 Configuring MG Data

MG configurations includes configuring MG registration information and configuring MG attribute.

In NGN, MG and MGC are separated devices. IAD108 acts as an MG, and the MG attribute describes the connection information between IAD108 and MGC.

4.5.1 Task List

Table 4-10 Task list of configuring MG data

Operation	Command
1. Configure MG registration information	**mg register-mode** { **private** | **standard** } [**register-key** *keyword* **password** *password*] **mg register-key** *keyword* [**password** *password* **register-mode** { **private** | **standard** }]
2. Configure MG attribute (mandatory)	**mg attribute** { **port** *port* | **code** *code* | **transfer** *transfer* | **domain-name** *domain-name* | **local-name** *local-name* | **mgcip** *mgcip* | **mgcport** *mgcport* | **mgc-domain-name** *mgc-domain-name* }

4.5.2 Configuring MG Registration Information

To prevent illegal MG from registering on MGC, start registration authentication function on the MG. Operate as follows:

1) Use command **mg register-mode** to set the registration mode of IAD108 as “standard” or “private”.

2) Use command **mg register-key** to configure registration key on the IAD108. The registration key configured on the IAD108 must be the same as that configured on the MGC. The registration key is a character string with 8–31 characters, and it is optional.

Note:

When configure the MG registration key, take the one set on MGC as the standard key. Otherwise, the MG cannot register successfully.

Example: Configure the IAD108 to register the MGC in standard mode. The registration key on the MGC is “iad108register”, and protection password is “iad108password”. After configuration, check as follows:

```
IAD2000(config)#mg register-mode standard
{ <cr>|register-key<K> }:

Command:
                mg register-mode standard
IAD2000(config)#mg register-key iad108register password
iad108password
{ <cr>|register-mode<K> }:

Command:
                mg register-key iad108register password
iad108password
```

```
IAD2000(config)#show mg register-info
{ <cr>|password<K> }:

Command:
                show mg register-info
  Mg register mode: Standard
  Mg register key: iad108register
  AuthMGID:iad16.com
IAD2000(config)#
```

The command used to configure the MG registration information is listed in Table 4-11.

Table 4-11 Command used for configuring MG registration information

Operation	Command
Query registration key of MG interface	IAD2000>**show mg register-info**

4.5.3 Configuring MG Attribute

MG attribute of the IAD108 is very important and must correctly configured. Otherwise, the IAD108 cannot register to the MGC.

I. Command format

In global config mode, you can use the following command to configure MG attribute:

mg attribute { **port** *port* | **code** *code* | **transfer** *transfer* | **domain-name** *domain-name* | **local-name** *local-name* | **mgcip**

mgcip | **mgcport** *mgcport* | **mgc-domain-name** *mgc-domain-name* }

The configuration result can be check by using command **show mg attribute** in user mode.

⚠ **Caution:**

IP address of the IAD108 should be configured before configuring MG attribute. To do this, carry out command **ip address** *ip-address net-mask def-gateway* in global config mode. If the IP address is configured later than the MG attribute, the IAD108 will register to the MGC again.

For the data that should be kept consistent on the IAD108 and MGC, refer to Table 4-2.

II. Parameter descriptions

The parameters of the commands used to configure MG attribute are listed in Table 4-12.

Table 4-12 Parameters of the commands used to configure MG attribute

Parameter	Description
code	Coding type, which can be text (text coding) or binary (binary coding). The coding type should be negotiated with the MGC, and should be identical with that configured on the MGC. The H.248 protocol supports the above two coding types, while the MGCP only supports the text coding. The system supports text coding by default.
domain-name	The name of MG, that is the domain name of the media gateway. It must be configured and kept identical with that configured on the MGC.
mgc-domain-name	MGC domain name, rangin 1–60 characters. It must be consistent with that configured on MGC. When IAD108 registers to the MGC, it first searches the MGC according to the domain name. If failed, register to the MGC according to the MGC IP address. The MGC domain name can be deleted with command **no mg attribute mgc-domain-name**.
local-name	Local MG terminal name. It is mandatory and should be kept identical with that configured on the MGC. This parameter is used only in MGCP.
mgcip	IP address of MGC.
mgcport	Port number of the MGC's transport layer protocol, determined by the configuration on MGC. With the MGCP, there is only text coding, and the default port number is 2727. The system's default port number is 2727
port	Port number of the MG transmission layer protocol. With the H.248 protocol, the protocol port number is related to the coding type, and the default port number is 2944 (text coding) or 2945 (binary coding). With the MGCP, there is only text coding, and the default port number is 2427.The system's default port number is 2427.

Parameter	Description
transfer	Transmission protocol type, which can be Transmission Control Protocol (TCP), User Datagram Protocol (UDP) or Simple Control Transmission Protocol (SCTP). MGCP only supports UDP. The system's default is UDP.

III. Usage example

Example: Configure the MG data as follows.

- Domain name of the MG interface as "huawei.com"
- MG domain name as "iad108.com"
- MG interface name as "aaln"
- IP address of MGC as "210.11.180.18"
- Other parameters adopt the system's default values.

```
IAD2000(config)#mg attribute domain-name iad108.com
local-name aaln mgc-domain-name huawei.com mgcip
210.11.180.18
{ <cr>|port<K>|mgcport<K>|code<K>|transfer<K> }:

Command:
                mg attribute domain-name iad108.com
local-name aaln mgc-domain-name huawei.com mgcip
210.11.180.18
IAD2000(config)#
```

After the configuration has been finished, you can use the command **show** in user mode to check the configuration result.

```
IAD2000(config)#show mg attribute
  ------------------------------------------------
```

```
    MGID          Protocol       Codetype       transmode
    0               MGCP           text            UDP
    MGIP          MGport         MGCIP          MGCPort
    172.21.100.16   2427           210.11.180.18   2727
    local-name                   Domain-name
    aaln                          iad108.com
    MG State                     MGC-Domain-Name
    MG wait ack                   huawei.com
    ------------------------------------------------
IAD2000(config)#
```

The command used to configure MG attribute is listed in Table 4-13.

Table 4-13 Command related to configure MG attribute

Operation	Command
Delete MGC domain name	IAD2000(config)#**no mg attribute mgc-domain-name**

4.6 Configuring Voice User Data

The voice access services provided by IAD108 can be divided into two types:

- Ordinary user service, in which the voice channels are selected at random instead of being designated. The establishment of voice channel is controlled by the MGC.
- Semi-Permanent Connection (SPC) service, in which the voice channels are dedicated and fixed. The establishment of the voice channel is not controlled by the MGC. Instead,

it is established by the related commands given from the command line or the NMS.

4.6.1 Configuring Ordinary Voice User

Ordinary voice users can be easily added according to the IAD108 user ports. You can use the command **show mguser** in user mode to check whether the system's default configurations meet the requirements.

Note:

No. 0–7 user ports of the IAD108 have been configured with default voice users according to general requirements. If there is no special requirements, use the default configurations.

I. Command format

You can use the following command in global config mode to add an ordinary voice user.

mguser add *portid* { **telno** *telno* | **mgtelno** *mgtelno* | **priority** *priorityflag* | **leaveword** *leavewordflag* | **terminalid** *terminalid* }

II. Descriptions of parameters

Parameters of the commands are listed in Table 4-14.

Table 4-14 Parameters of the commands used to configure voice users

Item	Description
portid	Port number. The ports are numbered from 0 and the value range is 0–7.
telno	Telephone number. It can be a different number from that configured on the MGC, and it is OK if you do not configure this number. The telephone numbers of the user ports on the IAD108 are assigned by the MGC.
mgtelno	Telephone number inside the IAD108. This number is determined by the IAD108, and there is no restrictions on the value. You can decide by yourself whether to configure this number or not.
priority	Flag of priority level for the access user. The value can be 0, 1 or 2, indicating respectively the high, medium or low priority. The default priority is “low”.
leaveword	Whether support the leave word function of the access user. The value can be 0 or 1, indicating “support” and “no support” respectively. The configuration should be the same as that on the MGC. By default, this function is not supported.
terminalid	Terminal ID, ranging 0–8.

Note:

- *telno* and *leaveword* are decided by the configuration on the MGC. On the IAD108, only a kind of record mode is configured to facilitate management and query.
- When adding or deleting users in batch, values of parameters *telno* and *mgtelno* are that of *startuser* plus 1.

III. Related commands

Table 4-15 Related commands

Operation	Command
Batch-adding access users	IAD2000config)#**mguser batadd startuser** *startuser* **enduser** *enduser* { **telno** *telno* | **mgtelno** *mgtelno* | **priority** *priority* | **leaveword** *leaveword* | **terminalid** *terminalid*}
Deleting an access user	IAD2000(config)#**mguser del** *portid*
Batch-deleting MG users	IAD2000(config)#**mguser batdel startuser** *startuser* **enduser** *enduser*
Modifying the access user data	IAD2000(config)#**mguser modify** *portid* **telno** *telno* **mgtelno** *mgtelno* **priority** *priority* **leaveword** *leaveword*
Terminating service forcibly	IAD2000(config)#**endservice** *portid*
Restarting the service	IAD2000(config)#**startservice** *slotid/portid*
Displaying the access user data	IAD2000(config)#**show mguser** [*portid*]

IV. Usage example

1) Query the system's default user configuration.

```
IAD2000(config)#show mguser
{ <cr>|portid<U><0,7> }:

Command:
```

```
                show mguser

-------------------------------------------------------
-
   Port MGID TerminalID Priority LWDflag Telno MGtelno

-------------------------------------------------------
-
   0     0           0       Low       No             -
-
   1     0           1       Low       No             -
-
   2     0           2       Low       No             -
-
   3     0           3       Low       No             -
-
   4     0           4       Low       No             -
-
   5     0           5       Low       No             -
-
   6     0           6       Low       No             -
-
   7     0           7       Low       No             -
-

-------------------------------------------------------
-
IAD2000(config)#
```

2) Delete the port 3 user, and set the priority of the newly added port 3 user to the highest level.

```
IAD2000(config)#mguser del 3
  Are you sure to delete the port data? (Y|N)y
IAD2000(config)#mguser add 3 priority 0
{   <cr>|terminalid<K>|telno<K>|mgtelno<K>|leaveword<K>
}:

Command:
                mguser add 3 priority 0
  Subscriber data are being generated. Please wait...
  Command executed. Data of 1 users added successfully!
```

3) Query the newly added port 3 user.

```
IAD2000(config)#show mguser 3

-------------------------------------------------------
-
   Port MGID TerminalID Priority LWDflag Telno MGtelno

-------------------------------------------------------
-
   3     0           3      High       No             -
-

-------------------------------------------------------
-
IAD2000(config)#
```

4.6.2 Configuring SPC Service

I. Overview of SPC service

Without presence of an MGC, the SPC can be established by the commands issued from the command line terminal or NMS, in order to set up an SPC between the ports of two IAD108s, or between different ports of the same IAD108. In SPC, the voice channels are fixed and dedicated, so that the service demands and communication quality of important users can be guaranteed.

There are two kinds of SPCs:

- IP SPC, which is established between the IAD108 and another IAD.
- Internal SPC, which is established between the ports of the same IAD108.

On the same user port, you can configure either the ordinary access user service or the SPC service. In case both services are configured on the same user port, the SPC service will have a higher priority. To enable the ordinary user service on this port, you must release or delete the SPC service data on this port.

II. Related commands

The commands used for configuring SPC are listed in Table 4-16.

Table 4-16 Commands used for configuring SPC

Operation	Command
Add an SPC	IAD2000(config)#**spc add start** *portid* { **end** *portid* | *local-port remote-ip remote-port* } [**name** *spcname*]
	To configure internal SPC, use command **spc add start** *portid* **end** *portid* [**name** *spcname*]. To configure IP SPC, use command **spc add start** *portid local-port remote-ip remote-port* [**name** *spcname*].
	When an IP SPC is established between equipment A and B, the *local-port* at A must be consistent with the *remote-port* at B, and the *local-port* at B must be consistent with the *remote-port* at A.
Modify an SPC	IAD2000(config)**spc modify** *connectid* {**start** *portid* | **end** *portid* | **name** *spcname* | **local-port** *local-port* | **remote-ip** *remote-ip* | **remote-port** *remote-port* }
Set the data signal processor (DSP) channel parameter of IP SPC	IAD2000(config)**spc dsp-channel** *connectid dsp-voice-code dsp-ece dsp-sce dsp-rtppacket-interval*
Delete an SPC	IAD2000(config)**spc delete** { **connectid** *connectid* | **from-connectid** *fromid* [**to-connectid** *endid*] }
Release an SPC	IAD2000(config)**spc release** { **connectid** *connectid* | **from-connectid** *fromid* [**to-connectid** *endid*] }
Recover an SPC	IAD2000(config)**no spc release** { **connectid** *connectid* | **from-connectid** *fromid* [**to-connectid** *endid*] }
Show the SPC information	IAD2000>**show spc** [**connectid** *connectid* | **from-connectid** *fromid* [**to-connectid** *endid*]]

If an SPC is successfully added, system will return its index number. This index can be used for modifying, deleting, releasing, establishing and querying the parameters of SPC.

When adding an IP SPC, you must configure the DSP channel information for the SPC, and the configuration on both ends of the SPC must be the same.

By releasing and establishing an SPC, you can manage the SPC dynamically. When an SPC is needed, you can execute command **no spc release** to establish it, and execute command **spc release** to release it when it is not needed. Different from deleting an SPC, this command only releases the SPC and the configuration data is not really deleted.

Caution:

If you delete an SPC, its configuration data will get lost. If you enter the *fromid* of an SPC without entering the *endid*, all the SPCs after the *fromid* will be deleted. So you must use the **spc delete** command with caution.

III. Descriptions of parameters

The parameters of the commands used to configure SPCs are listed in Table 4-17.

Table 4-17 Parameter of the commands

Item	Description
portid	Port number
spcname	Name of an SPC in a character string, the length is between 1 to 8 characters.
remote-ip	IP address of remote MG
local-portt	Local Real-time Transport Protocol (RTP) port number, used to identify different voice channels. Its value ranges [50000, 50124], and must be a multiple of 4. When adding an IP SPC, the DSP parameters at both ends must be configured consistently. For example, if IAD1 uses No. 50000 channel, IAD2 uses No. 50004 channel, you should configure *local-port*/r*emote-port* on IAD1 as 50000/50004, and 50004/50000 on IAD2.
r*emote-port*	Remote Real-time Transport Protocol (RTP) port number, ranging 0–65535.
connectid	Index of an SPC
fromid	Start index of an SPC
endid	End index of an SPC. In you do not input the *endid*, the last index will be taken by default.

Caution:

When adding an IP SPC, the DSP port parameters at both ends must be configured consistently, including voice coding type (*dsp-voice-code*), echo cancellation switch (*dsp-ece*), silence compression switch (*dsp-sce*) and RTP packetization interval (*dsp-rtppacket-interval*). The DSP port parameters of IAD108 can be set with command **mg system-parameter**. For details, refer to Section 5.3.1.

IV. Usage example

1) Add an internal SPC, including IAD108's port 0 and port 3, with the connection name as "iadspc".

```
IAD2000(config)#spc add start 0 end 3 name iadspc
  Adding SPC succeeded! The SPC index is: 0.
IAD2000(config)#
```

The internal SPC is created successfully, and the system returns the index "0".

2) Add an IP SPC

Establish an IP SPC between IAD108A and IAD108B. The data settings are as follows.

- IP address of IAD108A is 210.11.252.19.
- IP address of IAD108B is 210.11.10.26.
- The IP SPC connects port 6 of IAD108A and port 1 of IAD108B.
- The RTP port number at IAD108A is 50000.
- The RTP port number at IAD108B is 50004.

Operate as follows:

```
IAD108A(config)#spc add start 6 50000 210.11.10.26 50004
name ipspc
  Adding SPC succeeded! The SPC index is: 0.
IAD108A(config)#
```

After the IP SPC is successfully created on IAD108A, the system returns the index “0”.

```
IAD108B(config)#spc add start 1 50004 210.11.252.19 50000
name ipspc
  Adding SPC succeeded! The SPC index is: 0.
IAD108B(config)#
```

After the IP SPC is successfully created on IAD108B, the system returns the index “0”.

3) Show the configuration results on both IAD108A and IAD108B.

Operation on IAD108A:

```
IAD108A(config)#show spc
{ <cr>|connectid<K>|from-connectid<K> }:

Command:
                show spc

-------------------------------------------------------
-
  index   state   type   Port  Port  name
  0       Normal  IP-SPC   6  -     ipspc
IAD108A(config)#
```

Operation on IAD108B:

```
IAD108B(config)#show spc
{ <cr>|connectid<K>|from-connectid<K> }:


Command:
                show spc


-------------------------------------------------------
-
  index   state   type   Port  Port  name
  0       Normal  IP-SPC   1  -    ipspc
IAD108B(config)#
```

4.7 Configuration Examples of IAD108

4.7.1 Description of Networking

I. Networking Diagram

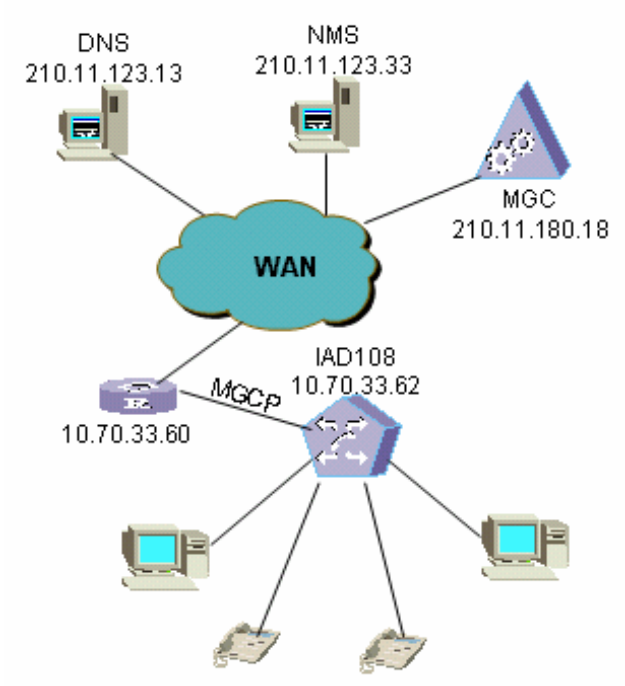


Figure 4-2 Networking for configuration example

II. Service requirements

1) Fixed IP address has been configured for IAD108.
2) The system time is configured as the same as that of MGC.
3) IAD108 is managed by IADMS, and it registers to IADMS when it is started.
4) DNS client is started on IAD108.

Configure ordinary access user service.

5) All the ports on IAD108 provide ordinary voice user service.

Configure SPC service.

6) Implement the internal SPC service between No.1 and No.3 ports of IAD108. Implement the IP SPC between No.4 port of IAD108 and other IAD devices.

4.7.2 Collecting Data

The items that need to plan IP addresses are listed in Table 4-18.

Table 4-18 Table of IP address allocation

Item	IP address
IP address of IAD108	10.70.33.62
IP address of IAD108's default upstream gateway.	10.70.33.60
IP address of MGC	210.11.180.18
IP address of IADMS	210.11.123.33
IP address of DNS	210.11.123.13

Parameters for interworking IAD108 with MGC are listed in Table 4-19.

Table 4-19 Parameters for interworking IAD108 with MGC

Data that should be configured on MGC	Data that should be configured on IAD108
IP address of IAD108: 10.70.33.62	IP address of MGC: 210.11.180.18
UDP port number (mgcport): 2427	Port number of transport layer protocol (port): 2727
Type of control protocol: MGCP	Type of control protocol: MGCP
Encoding type: text	Encoding type: text
Type of transmission protocol: UDP	Type of transmission protocol: UDP
IAD108 domain name: huawei.com	IAD108 domain name: huawei.com
IAD108 interface name: aaln	IAD108 interface name (local name): aaln

4.7.3 Configuring Basic Information of IAD108

I. Configuring IP Address of Equipment

Configuring the fixed IP address of IAD108 as 10.70.33.62, subnet mask as 255.255.255.0, and the default gateway as 10.70.33.60.

```
IAD2000(config)#ip address 10.70.33.62 255.255.255.0
10.70.33.60
  Changing net parameter may affect current service,
continue?[Y|N]:y
  Command executing, please wait...
```

```
------------------------------------------------
  ip address     : 10.70.33.62
  subnetwork mask: 255.255.255.0
  default gateway: 10.70.33.60
------------------------------------------------
Begin            Register            to            IADMS
1 ......................................
 Time out when registering to IADMS 0
Begin            Register            to            IADMS
1 ......................................
 Time out when registering to IADMS 1
IAD2000(config)#
```

II. Configuring System Time

Configure the system time as 2004-08-13, 09:33:30

```
IAD2000(config)#clock set 09:33:30 2004-08-13
  Current date: 2004-08-13
  Current time: 09:33:30
IAD2000(config)#
```

III. Starting DNS Client

Start DNS client on IAD108, designating the DNS domain name of IAD108 as “tele.com”, and the IP address of DNS server as “210.11.123.13”. After that, query the execution result. The operations are as follows.

```
IAD2000(config)#dns domain-name tele.com
IAD2000(config)#dns server 210.11.123.13
{ <cr>|second<I> }:
```

```
Command:
                dns server 210.11.123.13
IAD2000(config)#show dns status
------------------------------------------------------
-
Domain name:tele.com
Server address:
210.11.123.13
------------------------------------------------------
-
IAD2000(config)#
```

IV. Adding IADMS

Configure the EID of IAD as “iad@huawei”.

```
IAD2000(config)#eid iad15@huawei
IAD2000(config)#
```

Configure the IP address of IADMS as 210.11.123.33.

```
IAD2000(config)#iadms 1 ip 210.11.123.33 get set trap 162
IAD2000(config)#
```

Configure IAD108 to register to IADMS when it is started.

```
IAD2000(config)#iadms 1 register enable
IAD2000(config)#
```

4.7.4 Configuring MG Attribute Data

Configure MG attribute data. The domain name of MG interface is “huawei.com”, and the interface name is “aaln”, and the IP address

of MGC is “210.11.180.18”. Other parameters adopt system default values.

```
IAD2000(config)#mg attribute domain-name huawei.com
local-name aaln mgcip 210.11.180.18
{ <cr>|port<K>|mgcport<K>|code<K>|transfer<K>|mgc-doma
in-name<K> }:

Command:
                mg attribute domain-name huawei.com
local-name aaln mgcip 210.11.180.18
IAD2000(config)#
```

When the configuration is finished, you can use the command **show** in user mode to check the configuration result.

```
IAD2000(config)#show mg attribute
  ------------------------------------------------
  MGID          Protocol       Codetype       transmode
  0               MGCP           text            UDP
  MGIP          MGport         MGCIP          MGCPort
  10.70.33.62     2427           10.71.37.105    2727
  local-name                     Domain-name
  aaln                           huawei.com
  MG State                       MGC-Domain-Name
  MG wait ack
  ------------------------------------------------
IAD2000(config)#
```

4.7.5 Configuring Voice User Data

I. Configuring Ordinary Voice User Data

Check the default configuration of the system to see whether it meet the need.

```
IAD2000(config)#show mguser
{ <cr>|portid<U><0,7> }:

Command:
                show mguser

-------------------------------------------------------
-
   Port MGID TerminalID Priority LWDflag Telno MGtelno

-------------------------------------------------------
-
   0     0           0       Low       No             -
-
   1     0           1       Low       No             -
-
   2     0           2       Low       No             -
-
   3     0           3       Low       No             -
-
   4     0           4       Low       No             -
-
   5     0           5       Low       No             -
```

```
-
   6     0           6       Low       No              -
-
   7     0           7       Low       No              -
-


------------------------------------------------------
-
IAD2000(config)#
```

For ordinary voice users, the above configurations can meet the need and no more configurations are needed.

II. Configuring SPC User Data

1) Add an internal SPC, which connects No.1 and No.3 ports of IAD108, and its name is “iadspc”.

```
IAD2000(config)#spc add start 1 end 3 name iadspc
  Adding SPC succeeded! The SPC index is: 0.
IAD2000(config)#
```

After the internal SPC is successfully created, index “0” will be returned.

2) Add an IP SPC.

- IP address of IAD108A is 10.70.33.62.
- IP address of IAD108B is 10.70.10.26.
- This IP SPC is established between No.6 port of IAD108 and No.1 port of IAD108B.
- RTP port number of IAD108A is 50000.
- RTP port number of IAD108B is 50004.
- The name of the SPC is “ipspc”.

```
IAD2000(config)#spc add start 6 50000 10.70.10.26 50004
name ipspc
  Adding SPC succeeded! The SPC index is: 1.
IAD2000(config)#
```

After the IP SPC is successfully established at IAD108A, the system returns index “1”.

```
IAD108B(config)#spc add start 1 50004 10.70.33.62 50000
name ipspc
  Adding SPC succeeded! The SPC index is: 0.
IAD108B(config)#
```

After the IP SPC is successfully established at IAD108B, the system returns index “0”.

3) After the configuration is finished, check the configuration results on IAD108A and IAD108B.

On IAD108A, operate as follows:

```
IAD2000(config)#show spc
{ <cr>|connectid<K>|from-connectid<K> }:

Command:
                show spc

-------------------------------------------------------
-
  index   state   type   Port  Port  name
  0       Normal  IAD-SPC  1  3    iadspc
  1       Fault   IP-SPC   6  -    ipspc
IAD2000(config)#
```

On IAD108B, operate as follows:

```
IAD108B(config)#show spc
{ <cr>|connectid<K>|from-connectid<K> }:

Command:
                show spc

-------------------------------------------------------
-
  index   state   type   Port  Port  name
  0       Normal  IP-SPC   1   -    ipspc
IAD108B(config)#
```

4.7.6 Saving Configuration Data

After configuration is finished, save the data with command **write**.

```
IAD2000(config)#write
  Command executing, please wait...
System starts to save configuration data, please wait a
moment......
The configuration data backup percent is: 100%
IAD2000(config)#
```

Chapter 5 Advanced Configuration

5.1 Configuring Common Attributes of Access User

The common attributes of access users and SPC users include: ringing and PSTN port attributes. These attributes can be defined or take the default values.

5.1.1 Configuring Ringing Mapping Record

I. Command Description

During the interaction of the MGC and the IAD108, they negotiates about the ringing type. Ringing mapping is to establish a corresponding relationship between the ringing type parameters that the MGC sends to the IAD108 and the ringing tones that the IAD108 provides.

Example:

Add the ringing mapping records to Hong Kong of mapping the ringing type parameter 22 of the MGC to the ringing tones of the IAD108. Map the cadence ringing tone to the Hong Kong ringing tone type 2 and the initial ringing tone to type 18. With such configuration, when the MGC sends the ringing type parameter 22 to the IAD108, the IADE(T) will adopt these two ringing tones.

```
IAD2000(config-if-mg-0)#mgringmode add 22 2 18
```

II. Related Commands

Table 5-1 lists the related commands.

Table 5-1 Related commands

Operation	Command
Add a ringing mapping record	IAD2000(config)#**mgringmode add** *mgcpara cadence initialring*
Delete a ringing mapping record	IAD2000(config)#**mgringmode delete** [*mgcpara*]
Modify the attributes of a ringing mapping record	IAD2000(config)#**mgringmode modify** *mgcpara* [**cadencering** *cadenc* | **initialring** *initialring*]
Query the attributes of a ringing mapping record	IAD2000>**show mgringmode attribute** [*mgcpara*]

III. Parameter Description

Table 5-2 lists the parameters in the related commands and their meanings.

Table 5-2 Parameter descriptions

Item	Description
mgcpara	The parameter identifier of the opposite end, ranging 0–255.
cadence	The type of cadence ringing, ranging 0–255. The default value is 0, that is, to adopt the normal ringing tone.
initialring	The type of initial ringing, ranging 0–255. The default value is 4, that is, to adopt the normal ringing tone.
ring-type	Self-defined ringing type, ranging 0–15. The system permits you to set 16 ringing types.

Note:

The data packet that the MGC sends to the IAD108 contains the ringing type parameter (whose value is the same as that of *mgcpara*), by which the IAD108 searches in the table of ringing mapping records, finds the matching *mgcpara* and then gets the corresponding ringing types of *cadencering* and *initialring*.

Take Hong Kong as an example, and add a ringing mapping record. Correspond the ringing type parameter 22 of MGC with the ringing types of IAD108, and adopt the Hong Kong ringing type 2 as the cadence ringing tone, and Hong Kong ringing type 18 as the initial ringing tone. In this way, when the MGC sends the ringing type parameter 22 to the IAD108, the IAD108 will use these two kinds of ringing type. The operation is as follows:

```
IAD2000(config)#mgringmode add 22 2 18
IAD2000(config)#
```

5.1.2 Configuring PSTN Port Attribute

The PSTN port attributes include: the volume which can be sent and received by the PSTN access user, whether pulse dialing is permitted at the PSTN port, and whether to provide polarity reversal charging at the PSTN port.

I. Configuring Polarity Reversal Charging

Polarity reversal charging is a way to realize “immediate charging” of the access user. The charging terminal (for example, user charging phone) with this function has charging data itself, so only the start and end time of the conversation is needed. The IAD108

identifies the start and end time of the conversation by the polarity reversal of the subscriber line to which the ASI board is connected, and in this way it realizes polarity reversal charging.

If the IAD108 coordinates with the MGC to send the polarity reversal signal, either the IAD or the MGC can be configured to control the polarity reversal signal. However, it is recommended to select the MGC, that is, to set system parameter 23 of the IAD to 0 and set the polarity reversal at the subscriber port to “reverse”. Surely, the IAD can also be selected according to the actual condition.

⚠ **Caution:**

When the IAD is set to control the polarity reversal charging signal, the subscriber polarity reversal parameter of the MGC must be set to “no”. Otherwise, there will be repeated charging.

If the IAD is set to control polarity reversal charging, the PSTN port has to be configured with polarity reversal charging as well as the system parameter 23 that controls the polarity reversal charging signal. To modify a system parameter, use the command **mg system-parameter.**

Example:

Configure the attributes of port 0: Set the gain type of the PSTN access user to 6 and enable pulse dialing and polarity reversal charging at the PSTN port.

```
IAD2000(config)#pstnport attribute set 0 6 enable reverse
```

```
{ <cr>|V21TimerLen<K> }:


Command:
                pstnport attribute set 0 6 enable reverse
  Data configuration succeeded!
IAD2000(config)#
```

Example:

Set the IAD to control the polarity reversal signal, use the following command. To make this successful, it must be ensured that the polarity reversal switch on the MGC is off.

```
IAD2000(config)#mg system-parameter 23 1
IAD2000(config)#
```

II. Configuring the Send and Receive Gains at the PSTN Physical Port

The send and receive gains at the PSTN physical port of the IAD108 are adjustable. Normally the volume of the talk can be greatly enhanced by adjusting the send and receive gain at the PSTN physical port of the IAD108.

- As recommended in the Chinese national standards, the send and receive gain of the local network is 0/-3.5 (that is, high gain) and that of the toll network is 0/-7.
- It is recommended in the foreign countries that the send and receive gain of narrowband transmission is both 0/-7.

Because the voice of the IAD108 is sent and received by RTP packets, which can be regarded as a group trunk, similar to the PCM trunk, it is recommended to set the send and receive gain of the subscriber physical port of the IAD108 to 0/-7 (that is, low gain).

Example:

Set the send and receive gain at port 0 of slot 1 to low gain.

```
IAD2000(config)#pstnport attribute set 7 9 disable reverse
{ <cr>|V21TimerLen<K> }:

Command:
                pstnport attribute set 7 9 disable reverse
  Data configuration succeeded!
IAD2000(config)#
```

III. Related Commands

Table 5-3 listed the related commands.

Table 5-3 Related commands

Operation	Command
Set the attributes of PSTN port	IAD2000(config)#**pstnport attribute set** *portid* [*voicegain pulse-dial pole*]
Batch set the attributes of PSTN port	IAD2000(config)#**pstnport attribute batset startuser** *portid* **enduser** *portid* [*voicegain pulse-dial pole*]
Display the attributes of PSTN port	IAD2000>**show pstnport attribute** [*portid*]

IV. Parameter Description

Table 5-4 lists all the parameters in the commands and their meanings.

Table 5-4 Parameters descriptions

Item	Description
portid	The number of the slot, ranging 0–7
portid	The start and end port numbers in the batch-adding commands, ranging 0–7. The start port number cannot be greater than the end port number.
voicegain	The gain type of the PSTN access user. The value of this parameter represents the voice volume sent and received at the PSTN port. The more the gain is, the louder the voice will be The gain is calculated in dB. The sum of the send and receive gain ranges 0–17. Value 0 means high gain, while 1 means low gain. If this parameter takes other values, it means the send gain and receive gain are different. The default value is high gain.
pulse-dial	Whether permit pulse dialing at the PSTN port. The value can be “enable” or “disable”. Default is “disable”.
pole	Whether the PSTN port provides polarity reversal function. The value can be “normal” or “reverse”. Default is “reverse”.

The values of the parameter *voicegain* are listed in Table 5-5.

Table 5-5 Values of the parameter voicegain

Parameter value	Send gain (dB)	Receive gain (dB)
0	3	3
1	3	0
2	3	-3.5
3	3	-7
4	3	-12
5	3	-8.5

Parameter value	Send gain (dB)	Receive gain (dB)
6	0	3
7	0	0
8	0	-3.5
9	0	-7
10	0	-12
11	0	-8.5
12	-3	3
13	-3	0
14	-3	-3.5
15	-3	-7
16	-3	-12
17	-3	-8.5

5.2 Configuring Parameters of Built-In LAN Switch

The chip of the built-in LAN Switch in the IAD108 accommodates six Ethernet ports, among which ports 1–3 are used by external users, port 6 is for internal use, and other ports are reserved. Ports 1–3 do not have MAC addresses, nor are they configured with IP addresses. They can be used by merely being connected to the Ethernet cable.

The functions of the LAN Switch ports are listed below:

- Being upstream ports of the IAD108.

Port 1 of the LAN Switch chip on the IAD108 is used as an upstream port.

- Accessing data subscribers.

Ports 2 and 3 of the LAN Switch chip on the IAD108 are used to access data subscribers.

5.2.1 Configuring Precedence of Voice Packets

I. Principle

The upstream packets of the IAD108 include data packets and voice packets. To ensure high quality of voice and to give precedence to voice packets, the voice packets must be separated from the data packets. The specific way is as follows: Configure VLAN tag and rather high precedence to voice packets on the IAD, and the packets will be separated at the upper network equipment (for instance, the LAN Switch).

In the example shown in Figure 5-1, the conditions are as follows.

When the voice packets are configured with VLAN tag and rather high precedence on the IAD, the LAN Switch A will forward the voice packets with the VLAN tag to the LAN Switch C through a special port (“tag” in the figure) and forward the voice packets without the VLAN tag to the LAN Switch B through another port (“distag” in the figure). In this way, the separation of voice and data packets is realized at the LAN Switch A.

Due to the rather high precedence configured to voice packets, the LAN Switch A will discard some data packets and forward the voice packets to the LAN Switch C when the network is blocked.

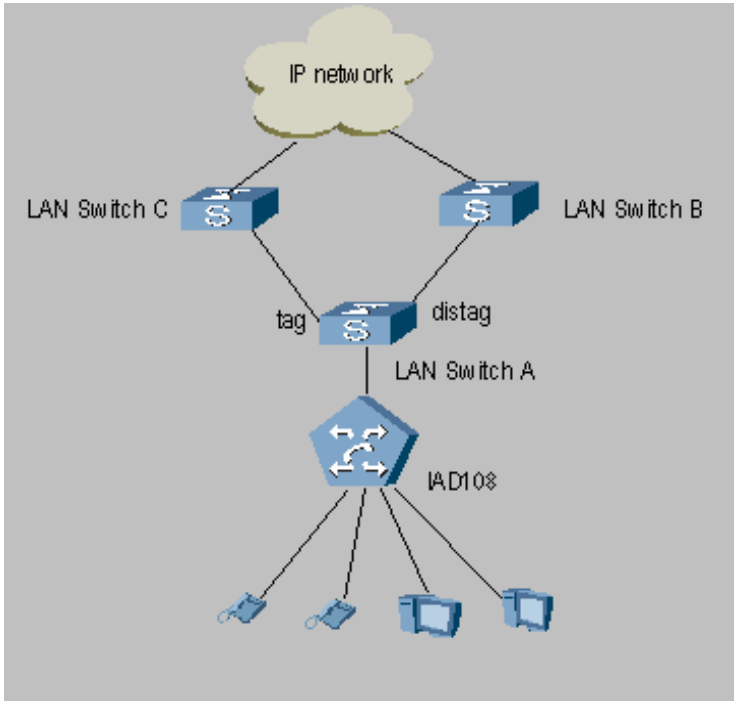


Figure 5-1 Networking for separating voice packets with VLAN tag and precedence

On the IAD108, only voice packets can be configured with VLAN tag and precedence. This is due to the flow direction of packets in the IAD. Figure 5-2 demonstrates the flow direction of packets in the IAD108.

Ports 1–3 are the ports for external use. Port 1 is used for upstream, ports 2–3 are used for accessing data user, port 6 is used for interface use, and ports 4 and 5 are reserved.

The CPU achieves configuration of VLAN tag and precedence to voice packets.

The upstream voice stream is first coded at the DSP, then transformed into voice packets at the CPU, and finally transmitted to the IP network through port 1 of the LAN Switch chip.

The upstream data stream is accessed through ports 2–3, and then transmitted to the IP network through port 1, without being processed at the CPU. Therefore, only voice packets can be configured with VLAN tag and precedence.

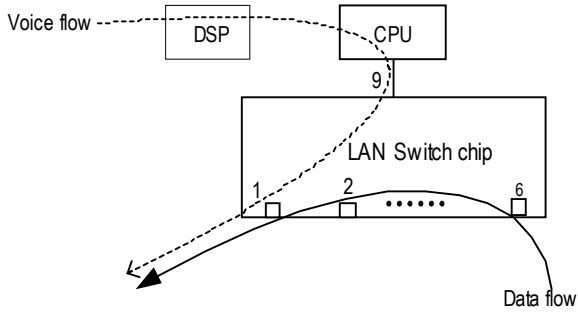


Figure 5-2 Flow chart of voice/data stream in the LAN Switch chip

II. Related Commands

Table 5-6 lists the related commands.

Table 5-6 Related commands

Operation	Command
Enable the VLAN tag function	IAD2000(config)#**tag** { **enable** | **disable** }

Operation	Command
Configure the VLAN tag and precedence	IAD2000(config)#**tag vlanid** *vlanid* **priority** *priority*
Configure the priortiy of ToS	IAD2000(config)#**tos** { **voice** | **other** } **priority** { **lowdelay** | **mincost** | **normal** | **reliability** | **throughput** }

Lists the parameters of the commands and their meanings.

Table 5-7 Parameter descriptions

Item	Description
vlanid	The number of VLAN, ranging 0–4095.
priority	The priority of VLAN, ranging 0–7. “0” has the highest priority.

III. Example

Example:

Enable the VLAN tag function on the IAD108, and configure VLAN tag to the upstream voice packets by setting VLAN ID to 0 and precedence to 3.

```
IAD2000(config)#tag enable
  Change the VLAN tag configuration will interrupt current
convesations, conitnue?[Y|N]:y
  Command executing, please wait...
-------------------------------------------------
  vlan tag function is enable
  vlan id        : 1
```

```
  vlan priority  : 7
-------------------------------------------------
IAD2000(config)#tag vlanid 0 priority 3
  Change the VLAN tag configuration will interrupt current
convesations, conitnue?[Y|N]:y
  Command executing, please wait...
-------------------------------------------------
  vlan tag function is enable
  vlan id        : 0
  vlan priority  : 3
-------------------------------------------------
IAD2000(config)#
```

Note:

When the VLAN tag is used to separate voice and data packets, it must be ensured that the upper network equipment (a router or a LAN Switch) also supports VLAN tag. When the VLAN tag function is enabled, the current calls will be affected.

Example:

Set ToS (Type of Service) of the voice packets to the highest reliability, and that of the other packets to the lowest cost.

```
IAD2000(config)#tos voice priority reliability
  Command executing, please wait...
-------------------------------------------------
  TOS of voice packets:  Maxmize reliability
  TOS of other packets:  Normal service
-------------------------------------------------
```

```
IAD2000(config)#tos other priority mincost
  Command executing, please wait...
-------------------------------------------------
  TOS of voice packets:  Maxmize reliability
  TOS of other packets:  Minimize monetary cost
-------------------------------------------------
IAD2000(config)#
```

Note:

The configuration of ToS is similar to that of VLAN tag. Whether the configuration is valid also depends on the upper IP equipment.

5.2.2 Other Configurations of LAN Switch

The commands used to configure and manage the LAN Switch ports of the IAD108 are listed in Table 5-8.

Table 5-8 Related commands

Operation	Command
Display the global configuration parameters	IAD2000(lanswitch)#**show lsw parameter**
Shut down/open the Ethernet port	IAD2000(lanswitch)#(**no**) **shutdown** *interface-num*
Set the duplex mode	IAD2000(lanswitch)#**duplex** *duplex-mode interface-num*
Display the configured data of port	IAD2000(lanswitch)#**show interface** [*interface-num*]*

Operation	Command
Set/cancel flow control	IAD2000(lanswitch)#(**no**) **flow-control** *interface-num**
Set the speed	IAD2000(lanswitch)#**speed** *speed-value interface-num*
Set the auto negotiation mode	IAD2000(lanswitch)#**negotiation-auto** *interface-num*
Configure VLAN	IAD2000(lanswitch)#**vlan** *vlan-id* **interface** *interface-num 1 interface-num 2 … interface-num 5*
Delete VLAN	IAD2000(lanswitch)#**no vlan** *vlan-id* [**interface** *interface-num 1 interface-num 2 … interface-num 5*]
Show VLAN configuration	IAD2000(lanswitch)#**show vlan** [*vlan-id*]
Set priority to a port	IAD2000(lanswitch)#**priority** *interface-num**
Remove priority of a port	IAD2000(lanswitch)#**no priority** *interface-num**
Set the monitoring port	IAD2000(lanswitch)#**monitor** *interface-num1* **observing-port** *interface-num2**
Cancel the configuration of the monitoring port	IAD2000(lanswitch)#**no monitor**
Display the monitoring port	IAD2000(lanswitch)#**show monitor-port**
Reset the port or the whole LAN Switch chip	IAD2000(lanswitch)#**reset** [**interface** *interface –num*] *
Clear the port statistics information	IAD2000(lanswitch)#**clear**

I. Parameter Description

Table 5-9 lists the parameters in the commands and their meanings.

Table 5-9 Parameter descriptions

Item	Description
interface-num, interface-num1 – interface-num8	LAN Switch port number of the IAD108, ranging 1–5. For the commands with a "*", its value ranges 1–6.
duplex-mode	The duplex mode of the LAN Switch port, being half or full. The two values represent the half duplex mode and full duplex mode respectively.
speed-value	The baud rate at the LAN Switch port, being 10 or 100. The two values represent 10 Mbit/s and 100 Mbit/s respectively.
vlan-id	VLAN ID, ranging 0–4095.

II. Examples

Example:

Set port 1 as work in full-duplex mode.

```
IAD2000(lanswitch)#duplex full 1
IAD2000(lanswitch)#
```

Set the rate of port 2 as auto negotiation, and the rate of port 3 as 100 Mbit/s.

```
IAD2000(lanswitch)#negotiation-auto 2
IAD2000(lanswitch)#speed 10 3
IAD2000(lanswitch)#
```

Note:

Ports of the IAD108 are 10/100Base-TX Ethernet ports, supporting baud rates of both 10 Mbit/s and 100 Mbit/s. They can work in half-duplex, full-duplex and auto negotiation modes. The default working mode is the auto negotiation mode.

Example:

Set port 2 with flow control and port 3 without.

```
IAD2000(lanswitch)#flow-control 2
IAD2000(lanswitch)#no flow-control 3
IAD2000(lanswitch)#
```

Example:

Set network ports 2 and 3 of the IAD108 into one VLAN, of which the VLAN tag is 1. Set network ports 4 and 5 into another VLAN, of which the VLAN tag is 2. In this case, the data users accessed from network ports 4 and 5 cannot visit those accessed from ports 2 and 3.

```
IAD2000(lanswitch)#vlan 1 interface 2 3
{ <cr>|interface-num<U><1,5> }:

Command:
                    vlan 1 interface 2 3
IAD2000(lanswitch)#vlan 2 interface 4 5
{ <cr>|interface-num<U><1,5> }:

Command:
                    vlan 2 interface 4 5
IAD2000(lanswitch)#
```

5.3 Configuring Software Parameters

The IAD provides the function of dynamic querying and configuring software parameters. This makes it possible to control the configurations and software flows by configuring the software parameters, so as to adjust to various application statuses. The software parameters of the IAD are classified into system software parameters and MG software parameters.

The system software parameters can be configured to adjust the noise, echo, jitter, and loudness of voice, the transmission mode of Fax/Modem, and the type of the MGC which networks with the IAD.

5.3.1 Configuring System Software Parameters

Table 5-10 lists the commands used for configuring system software parameters.

Table 5-10 Related Commands

Operation	Command
Configure system software parameters	IAD2000(config)#**mg system-parameter** *name value*
Display the configuration of system software parameters	IAD2000>**show mg system-parameter** [*name*]

Note:

When use command **show mg system-parameter** to query the software parameters (including system software parameters and MG software parameters), if no *name* is entered, all the software parameters of the system will be displayed. If *name* is entered, the value of designated software parameter will be queried.

value: Value of the system software parameter.

Name: the name of the system parameter, ranging 0–27. Each digit represents a specific parameter, as listed in Table 5-11.

Table 5-11 Values of parameter name and their meanings

Item	Description
0	Maximum number of subscribers that can be powered by remote power supply.
1	The lower limit for pressing hookflash, being 100 ms in both mainland China and Hong Kong. The default value is 100 ms.
2	The upper limit for pressing hookflash, being 300 ms in mainland China and 700 ms in Hong Kong. The default value is 300 ms.
3	The input gain of the DSP chip (IP->PCM). It ranges 2–64, corresponding to -31dB–0dB
4	The output gain of the DSP chip. It ranges 2–64, corresponding to -31dB–0dB.
5	The value of jitter buffer. This value ranges 0 ms – 150 ms and the default value is 60 ms.
6	This parameter is reserved for future use.
7	The default coding mode of the DSP channel, ranging 0–20. The value of 0 indicates G.711μ; 4 G.723High; 8 G.711A; 18 G.729; 20 G.723Low. The default value is 8 (G.711A).
8	The default EC switch of the DSP channel, ranging 0–1. The value of 0 indicates the switch is off; 1 on.
9	The default silence compression switch of the DSP channel. The value of 0 indicates the switch is off; 1 on.
10	The default interval for RTP packetization of the DSP channel, in unit of milliseconds. The value can be 10 ms, 20 ms, and 30 ms. The default value is 20 ms.

Item	Description	
11	Set whether the DSP channel needs the channel statistics information, ranging 0–1. The value of 0 indicates no; 1 yes.	
12	The transmission mode of the fax, ranging 0–4. The value of 0 indicates transparent transmission mode; 1 transparent transmission mode with fax related events reported; 2 T.38 V2; 3 T.38 V3; 4 T.38 transparent transmission mode.	
13	This parameter is reserved for future use.	
14	DTMF/MF code transmission over RTP, ranging 0–2.	0: Transparent transmission: The DTMF signal is packetized into RTP packets and transmitted.
		1: 2833 mode. The DTMF signal is transmitted in the RTP packets other than voice and message packets. The numbers can be sent and received normally even when the network is in bad condition.
		2: Outband transmission.
15	The flag for playing the howler tone. The value of 0 indicates the howler tone is not played; and 1 played.	
16	The flag for an overseas version. The value of 0 indicates China; 1 Hong Kong; 2 Brazil; 3 Egypt; and others are reserved.	
17	The flag for system self-check. The value of 0 indicates no self-check; 1 resetting the ports optionally; 2 resetting all free ports.	
18	The duration set at the timer for the dialing tone, in unit of seconds. The default value is 20 seconds.	
19	The duration set at the timer for the busy tone, in unit of seconds. The default value is 40 seconds.	
20	The duration set at the timer for the howler tone, in unit of seconds. The value of 0, the default value, indicates no timeout.	
21	Hair pin connection mode. It is reserved for future use.	

Item	Description	
22	The control mode for call waiting tone. 0: MGC controls it. 1: IAD controls it.	
23	The control mode for polarity reversal at the port. The value of 0 indicates the MGC controls the polarity reversal mode; 1 indicates the IAD controls this mode.	When the IAD108 is interworking with the ETG for usage in the IP AN (IP Access), this parameter must be set to 0, that is, the ETG controls the polarity reversal at the port.
24	The type of the MGC interworking with the IAD. It ranges 0–7, each of which represents one MGC type. The value of 0 indicates SoftX3000; 1 indicates the softswitch of Z; 2 of N; 3 of C; 4 of S; 5 of Sonus; 6 of ETG; 7 of Y. The default value is 0.	
25	Set whether to check the port number of the remote UDP. The value of 0 indicates no; 1 yes.	
26	Set whether to send the UPD checksum. The value of 0 indicates no; 1 yes.	
27	Amount of RFC2833 redundancy packets, ranging 0–4. Default value is 0.	

Example:

Set the upper and lower limits of pressing hookflas to meet the local standard. Take Hong Kong as an example, the upper limit is 700 ms, and the lower limit is 100 ms.

```
IAD2000(config)#mg system-parameter 2 700
IAD2000(config)#mg system-parameter 1 100
IAD2000(config)#
```

Note:

All the software parameters of the IAD108 have default values. Normally no modification is needed.

5.3.2 Configuring MG Software Parameters

Table 5-12 lists the commands used to configure MG software parameters.

Table 5-12 Related commands

Operation	Command
Configure MG software parameters	IAD2000(config)**mg software-parameter** *name value*
Display MG software parameters	IAD2000>**show mg software-parameter** [*name*]

value: Whether the terminal ID under the MG interface adopts layered configuration. 0 indicates yes, 1 no.

name: the name of the software parameter, ranging 0–6, whose meanings are listed in.

Table 5-13 Values of parameters name and value

name	value
0:It controls whether the ID of the terminal connected to the MG interface adopts layered configuration, ranging 0–1.	0: yes; 1: no.

name	value
1: It controls whether the current calls are held when the communication between the MGC and the MG is interrupted.	0: yes; 1: no.
2: It controls whether the calls are switched to the standby MGC when the communication between the MGC and the MG is interrupted.	The value of 0 indicates yes; 1 no, that is, the MG can only register on the active MGC.
3: It controls whether to stop sending the heartbeat message between the MGC and the MG.	The value of 0 indicates yes; 1 no.
4: It is the heartbeat duration.	It is in the unit of seconds, ranging 0–65,535 seconds.
5: It controls whether the wildcard is used at registration.	0: yes; 1: no.
6: Whether send long-duration call NTFY to MGC. This parameter is used when the IAD108 networks with O company's softswitch, because this softswitch cannot recognize the NTFY.	0: no; 1: yes.

Example:

Hold the current calls when the communication between the MGC and the MG is interrupted.

```
IAD2000(config)#mg software-parameter 1 0
IAD2000(config)#
```

5.4 Configuring Standby MGC

The IAD108 supports the MGC backup. When the active MGC is faulty, the IAD108 will register on the standby MGC automatically by the heartbeat detection or transaction reliability mechanism. Normally, it can also be manually switched to the standby MGC by the command line.

I. Configuration Steps

Before configuring the standby MGC, you have to use the command **mg interface-parameter** to switch on the MGC backup switch, which is off by default.

An IAD108 can be configured with only one backup MGC. The configuration can be made in two steps.

1) Turn on the MG software parameter switch

In global configuration mode, use command **mg software-parameter** to set the software parameter 2 to “0”, that is “can be switched to the backup MGC”.

2) Configure information of standby MGC

In global config mode, use command **mg backup** to configure the information for the backup MGC. For example, configure the backup MGC of the IAD108.

```
IAD2000(config)#mg software-parameter 2 0
IAD2000(config)#mg backup mgcip 1.1.1.1 mgcport 2222
mgc-domain-name huawei1.com
IAD2000(config)#show mg mgc
mgcip1:172.21.1.1       mgcport1:2727   mgc-domain-name1:
            Active
```

```
mgcip2:1.1.1.1                                    mgcport2:2222
mgc-domain-name2:huawei1.com


IAD2000(config)#
```

Table 5-14 lists the commands used to configure backup MGC.

Table 5-14 Related commands

Operation	Command
Turn on the switch for configuring backup MGC	IAD2000(config)**mg software-parameter** *name value*
Configure the standby MGC	IAD2000(config)**mg backup** {**mgcip** *mgcip* | **mgcport** *mgcport* | **mgc-domain-name** *mgc-domain-name* }
Query MG software parameter	IAD2000>**show mg software-parameterr**
Display the MGC	IAD2000>**show mg mgc**

Table 5-15 lists the parameters of the related commands and their meanings

Table 5-15 Parameter description

Item	Description
mgcip	The IP address or the domain name of the standby MGC. It must be consistent with that actually configured to the standby MGC. The domain name is a character string of 1–60 characters.
mgcport	The port number of transmission layer protocol. With MGCP, only text coding is supported and the default port number is 2727.

5.5 Configuring MGCP Parameters

I. Commands

You can define the MGCP parameters or just adopt the default values for them. It is recommended to adopt the default values. If you are to modify these parameters, use the following command to operate in the global config mode.

Table 5-16 lists the related command.

Table 5-16 Related commands

Operation	Command
Configure MGCP parameters	IAD2000#**mgcp** { **maxRetranTimer** *MaxRetranTimerval* | **retrantimerSeedflag** *RetranTimerSeedFlagVal* | **retrantimerSeed** *RetranTimerSeedVal* | **retransuspicionThreshold** *RetranSuspicionThresholdval* | **retrandisconnectThreshold** *RetranDisconnectThresholdVal* | **provRspflag** *ProvRspFlagVal* | **provRsptimer** *ProvRspTimerVal* | **provRspdelay** *ProvRspDelayVal* | **atMostOnceflag** *AtMostOnceFlagVal* | **atMostOncetimer** *AtMostOnceTimerVal* }
Display the MGCP version and parameters	IAD2000>**show mgcp** {*ver* | *param*}

II. Parameter Descriptions

Table 5-17 lists the parameters of the related commands and their meanings.

Table 5-17 Parameter descriptions

Item	Description
AtMostOnceFlagVal	Set whether to enable the at_most_once function. This function means that when A receives a command, it execute it only once. In this way, such case can be avoided that A re-sends the packets to B when the response from B is being transmitted in the network, that is, a command is re-executed. The values can be 0 (false) or 1 (true), and the default value is 1.
AtMostOnceTimerVal	The duration set at the timer for the at_most_once function. B calculates the time from the point when it sends the response message. If it receives the sent again packets within the duration set for this parameter, it will discard them. The value cannot be larger than 60 seconds and the default value is 30 seconds.
MaxRetranTimerval	Maximum retransmission time. After a command is sent, if no response is received, this command will be sent again. If no response is received during the time set by *MaxRetranTimer*, this command will not be sent again. Default value is 30 seconds.
RetranTimerSeedFlagVal	Set whether to configure the retransmission algorithm initial seed value. The two choices are “TRUE” and “FALSE”. If it is set to “TRUE”, it indicates that the first retransmission duration is set to *RetranTimerSeed*; or else, it is fixed to 2 seconds.
RetranTimerSeedVal	The initial seed value of the retransmission algorithm. It cannot be larger than 30 seconds, and must work in coordination with the *RetranTimerSeedFlag.*
RetranSuspicionThresholdval	The retransmission suspicion threshold. It must be smaller than *RetranDisconnectThreshold.* If the times for re-sending a command exceeds this value, the system enters the suspicion status and checks the DNS address or tries other destination addresses.
RetranDisconnectThresholdVal	The retransmission disconnect threshold. It must be larger than the *RetranSuspicionThresholdval.* When a system enters the suspicion status, if the times for re-sending a command exceeds this value, the command will not be sent again.

Item	Description
ProvRspFlagVal	Set whether to send a temporary response. When A sends a command to B, if the command execution takes a long time, B will send a temporary response to A, confirming that it has received the command. This reduces the possibility for A to resend the command. The two values are 0 (false) and 1 (true), and the default value is 1.
ProvRspTimerVal	The duration set for the temporary response, from the point when B receives A's command to the point when it sends the temporary response. This value cannot be larger than 5 seconds, and the default value is 2 seconds.
ProvRspDelayVal	The duration set for the temporary response delay. This value must be smaller than 30 seconds, and the default value is 5 seconds. When A receives the temporary response, it prolongs the *MaxRetranTimer* by a duration of *ProvRspDelayval*.

🕮 Note:

All the above parameters are optional. When a parameter is not checked, it means to adopt the default value. It is recommended to modify these parameters with caution. Either A or B can be MGC or IAD108.

Example:

Set the maximum retransmission time as 20 seconds, and disable the at_most_once function.

```
IAD2000(config)#mgcp maxRetranTimer 20 atMostOnceflag 0
{ <cr>|RetranTimerSeedFlag<K>|RetranTimerSeed<K>|RetranS
uspicionThreshold<K>|Ret
ranDisconnectThreshold<K>|ProvRspFlag<K>|ProvRspTimer<K>
```

```
|ProvRspDelay<K>|AtMostO
nceTimer<K> }:

Command:
                mgcp maxRetranTimer 20 atMostOnceflag 0
Set MGCP parameter success
IAD2000(config)#
```

Chapter 6 ADSL Service Configuration

The IAD108 can provide ADSL services and implement broadband access services for data users through the ATM mode.

6.1 Creating Configuration Environment

Before using ADSL services of the IAD108, create a configuration environment for ADSL on the equipment, as follows:

- The hardware version of the CSP board is version D.
- The CSP board has been installed with an ADSL subboard.
- The CSP board has been installed with an ADSL jumper.

6.1.1 CSP Hardware Version

When using ADSL features of the IAD108, make sure that the hardware version of the CSP board is version D.

- In the global configuration mode, use the **show version** command for confirmation. Proceed as follows:

```
IAD2000(config)#show version
  Equipment type            : IAD108
  Main Board PCB version    : AG21CSPA VER.D
  xDSL Board PCB version    : APU.1
  Software version          : IAD2000V200R002B01D051
  BIOS version              : 1200
  SLIC version              : (U35-U38)015
  CPLD version              : (U16)200
  DSP version            : (U34) VoIP V100R003C01B020D013
IAD2000(config)#
```

In the above results, the version information in line “Main Board PCB version” is displayed as “AG21CSPA VER.D”. “CSPA” indicates that the CSP board in use is of type A and the IAD108 can only use the CSPA board. “VER.D” shows the hardware version.

The CSP hardware version is also marked on the board, as shown in Figure 6-1.

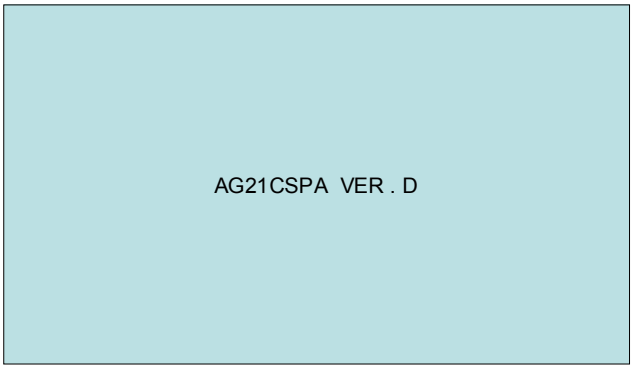


Figure 6-1 CSP hardware version

6.1.2 ADSL Subboard

To use ADSL features, select not only the CSP board of version D, but also the ADSL subboard. The subboard is installed in the corresponding slot of the CSP board, and processes ADSL services together with the CSP board.

- In the global configuration mode, use the **show version** and **show device** commands for confirmation. Proceed as follows:

```
IAD2000(config)#show version
  Equipment type            : IAD108
  Main Board PCB version    : AG21CSPA VER.D
```

```
  xDSL Board PCB version    : APU.1
  Software version          : IAD2000V200R002B01D051
  BIOS version              : 1200
  SLIC version              : (U35-U38)015
  CPLD version              : (U16)200
  DSP version           : (U34) VoIP V100R003C01B020D013
IAD2000(config)#
IAD2000(config)#show device
-------------------------------------------------
  FLASH size      : 8MB
  SDRAM size      : 32MB
  Up-link state   : Normal   Type : ADSL
  Pulse Code Modulation    : A Law
  DSP state       : Normal    DSP main frequency : 144MHZ
     DSP support codec algorithm : g.711&g.729&g.723
     DSP  software  version             :  (U34)  VoIP
V100R003C01B020D013
  EC state        : Normal
      Echo Return Loss     : 6DB
  Tone detector mode    : G164&G165
      Network Level Loss   : 0DB
      Non-Linear Processor : On
      Noise Transmit mode  : Transparent
  Lanswitch state : Normal
  SLIC0 State : Normal
      Total ports : 2 PSTN_PORT
  SLIC1 State : Normal
      Total ports : 2 PSTN_PORT
  SLIC2 State : Normal
```

```
        Total ports : 2 PSTN_PORT
    SLIC3 State : Normal
        Total ports : 2 PSTN_PORT
    Equipment ID    : 00-e0-fc-03-02-01
    RTC CHIP        : Not Exist
    ENVIRONMENT CHIP: Not Exist
    REMOTE POWER    : Supported but unused
--------------------------------------------------
IAD2000(config)#
```

In the above results of the **show version** command, the subboard type in line “xDSL Board PCB version” is displayed as “APU.1”. The information indicates that the CSP board has been installed with the ADSL subboard.

In the above results of the **show device** command, the uplink mode in line “Up-link state” is displayed as “ADSL”. The information indicates that the ADSL uplink mode is in use.

The ADSL subboard has three functions:

- ATM connection
- Internal Ethernet
- PPP dialing

The ADSL subboard is connected to the network through two interfaces. One interface connect the DSLAM through the ATM uplink of the subboard. The other interface connects the uplink Ethernet port of the IAD through the Ethernet port of the subboard.

I. ATM Connection

To connect the DSLAM through a subboard, first configure the ATM attribute on the ADSL subboard.

The ATM configuration includes the following four steps:

- Creating an ATM interface
- Creating a VC interface
- setting a VCI/VPI value
- Setting an encapsulation mode (optional)

By default, the ATM interface has been created and can be checked through related commands. Check beforehand if the ATM interface has been configured. If not, create the ATM interface.

II. Internal Ethernet

The default Ethernet segment of the ADSL subboard is 192.168.1.0. The IP address of the subboard is 192.168.1.1.

Inside the Ethernet, the subboard provides the HTTP and Telnet maintenance modes. So long as the IP addresses of the PC and the subboard are in the same network segment, you can log in to the subboard through the two modes and then configure it, or configure it with IAD command lines.

When the subboard is configured through HTTP/Telnet or IAD command lines, the IP addresses of the console have different restrictions, as listed below.

- When the subboard is configured through HTTP/Telnet, the IP address of the PC must be configured above 192.168.1.4, because 192.168.1.1–192.168.1.3 have been reserved by the subboard.
- When the subboard is configured through IAD command lines, there is no restriction for the IP address of the IAD.

III. PPP Dialing

The ADSL subboard can also complete the PPP dialing. During the dialing, the ADSL subboard works in the non-bridging mode and initiates the PPP connection. Configure a user name with a password for the PPP dialing on the ADSL subboard.

In addition, the ADSL subboard can provide the NAT service and serve as a DHCP server or a router. Basically, no configuration is needed for the use of the ADSL subboard in the Ethernet. If needed, you can configure the DHCP address pool and routing information.

6.1.3 Connecting Uplink Interface

After all hardware for ADSL applications is installed, you can connect the IAD108 uplink interface, to implement the physical connection between the IAD108 and upper equipment.

When the IAD108 provides ADSL services, it is connected to the uplink device only through the RJ-11 telephone interface in the ADSL mode. The uplink Ethernet port on the back panel can only be used as the RJ-11 telephone interface.

6.1.4 Connecting Downlink Interface

Compared with the connection of the downlink interface of the FE uplink mode, that of the ADSL uplink mode has no change. The two RJ-45 network ports on the back panel can only be connected to the PC. The eight RJ-11 POTS interfaces can only be connected to the user telephone.

Note:

For the IAD108 that provides ADSL services, all hardware has been configured at delivery. All you need to do is pay attention to the selection of the uplink mode of the RJ-11 telephone line interface, and the correct connection of the downlink PC or user telephone.

6.1.5 Example of Configuration Environment

Figure 6-2 shows the configuration environment of the IAD108 for ADSL applications.

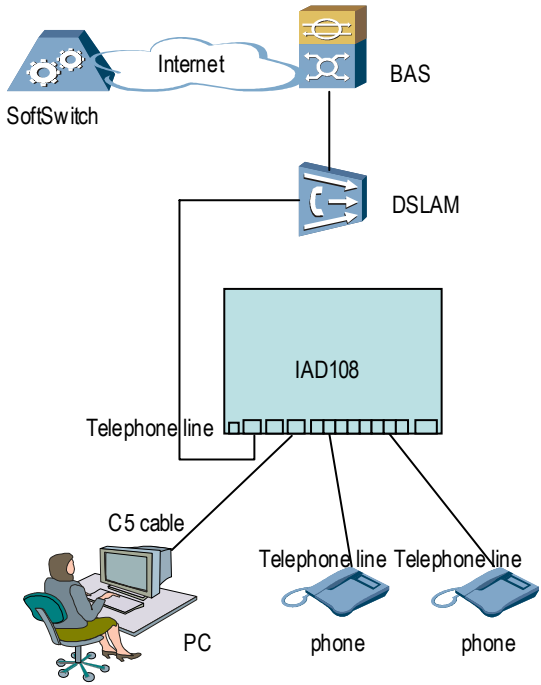


Figure 6-2 ADSL configuration environment

6.2 ADSL Configuration Commands

The ADSL configuration is performed on the ADSL subboard. According to the keywords, the command lines of the ADSL subboard can be divided into three types:

- Create
- Modify
- Get

The ADSL configuration commands provide the help system. The method is to add "**help**" to the end of the commands. You can query related command lines and function descriptions, such as "**adsl create help**" and "**adsl create atm help**".

In practical applications, the ADSL configuration commands are classified into the following categories:

- ATM related commands
- PPP related commands
- EoA related commands
- Bridging related commands

6.2.1 ATM Related Commands

Table 6-1 shows commands related to ATM.

Table 6-1 Commands related to ATM

Operation	Command and mode
Create an ATM interface	IAD2000(diagnose)%%**adsl create ATM interface ifname** *name* **maxvc** *decvalue*
Query the ATM interface information	IAD2000(diagnose)%%**adsl get ATM interface ifname** *name*
Query the DSL state information	IAD2000(diagnose)%%**adsl get dsl stats curr**
Query the AAL5 state information	IAD2000(diagnose)%%**adsl get atm aal5 stats**
Query the ATM VC information	IAD2000(diagnose)%%**adsl get atm vc intf**
Enable/Disable an ATM interface	IAD2000(diagnose)%%**adsl modify ATM interface ifname** *name* { **enable** | **disable** }

Operation	Command and mode
Modify a VPI/VCI	IAD2000(diagnose)%%**adsl modify atm vc intf ifname** *name* **vpi** *decvalue* **vci** *decvalue*
Modify the ATM encapsulation mode	IAD2000(diagnose)%%**adsl modify atm vc intf ifname** *name* { **vcmux** | **llcmux** | **none** }

6.2.2 PPP Related Commands

Table 6-2 shows commands related to PPP.

Table 6-2 Commands related to PPP

Operation	Command and mode
Create a PPP interface	IAD2000(diagnose)%%a**dsl create ppp intf ifname** *name* **lowif** *name* **ppoe**
Create the authentication related to the PPP interface	IAD2000(diagnose)%%**adsl create ppp security ifname** *name*
Delete all the PPP interfaces	IAD2000(diagnose)%%**adsl delete ppp intf**
Delete a specified PPP interface	IAD2000(diagnose)%%**adsl delete ppp intf ifname** *name*
Modify the PPP authentication mode	IAD2000(diagnose)%%**adsl modify ppp security ifname** *name* { **chap** | **pap** }
Modify the PPP account password	IAD2000(diagnose)%%**adsl modify ppp security ifname** *name* **login** *name* **passwd** *name*
Modify the PPP startup mode	IAD2000(diagnose)%%**adsl modify ppp intf ifname** *name* { **start** | **stop** | **startondata** }
Query the related information of the PPP	IAD2000(diagnose)%%**adsl get ppp intf**

Operation	Command and mode
Query the IP information of the PPP	IAD2000(diagnose)%%**adsl get ppp ipinfo**
Query the PPP security configuration	IAD2000(diagnose)%%**adsl get ppp security**
Query the PPP connection information	IAD2000(diagnose)%%**adsl get ppp lstatus**

6.2.3 EoA Related Commands

Table 6-3 shows commands related to EoA.

Table 6-3 Commands related to EoA

Operation	Command and mode
Create an EoA interface	IAD2000(diagnose)%%**adsl create eoa intf ifname** *name* **lowif** *name*
Query the EoA interface information	IAD2000(diagnose)%%**adsl get eoa intf**

6.2.4 Bridging Related

Table 6-4 shows commands related to bridging.

Table 6-4 Commands related to bridging

Operation	Command and mode
Set the bridging in the non-PPP mode	IAD2000(diagnose)%%**adsl create bridge port intf ifname** *name*
Delete the bridging mode	IAD2000(diagnose)%%**adsl delete bridge port intf ifname** *name*

Operation	Command and mode
Query a bridging port	IAD2000(diagnose)%%**adsl get bridge port intf**

6.3 Bridging Mode

6.3.1 Introduction to Bridging Principles

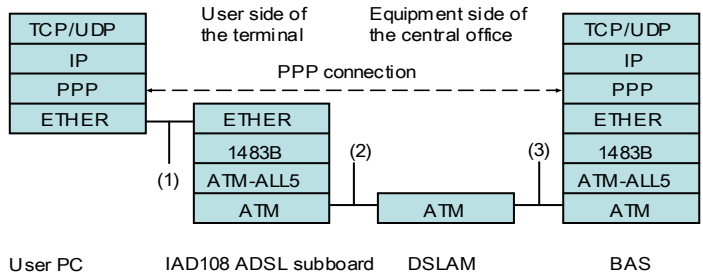
In the bridging mode, the ADSL subboard functions only as a bridge. When data packets pass the ADSL subboard, the subboard only encapsulates the packets to ATM cells. It transmits data stream transparently, just like a bridge.

In the bridging mode:

- The user PC or the IAD108 can initiate the PPP dialing. If the IAD108 initiates the dialing, the IAD108 can access the network. If the PC initiates the dialing, the PC can access the network.
- If the PC initiates the PPP dialing, it must be first installed with the PPP dialing software, and then configured with the user name and password of the PPP dialing. If the IAD108 initiates the PPP dialing, it can be directly configured with the user name and password of the PPP dialing.
- When the PC initiates the PPP connection, that is, the PC accesses the network, one ADSL subboard can connect multiple PCs. Each PC must have its own user name and password, to establish independent PPP connection to the ISN8850.
- The PPP connection in the bridging mode locates between the user PC and the BAS (such as Huawei's ISN8850) of the

upper network. The ADSL subboard only transmits layer 2 messages transparently as a bridge.

When the IAD108 networks with the upper DSLM (such as Huawei's MA5100) and BAS (such as ISN8850), and provides ADSL services, and the ADSL subboard works in the bridging mode, the protocol stack is as shown in Figure 6-3.



(1): Network cable/Ethernet packet (2): PSTN telephone line/ATM cell
(3): Optical fiber/ATM cell

Figure 6-3 Protocol stack in the bridging mode

6.3.2 Networking Examples

Figure 6-4 and Figure 6-5 show networking examples of the IAD108 ADSL subboard, in the bridging mode.

- In Figure 6-4, the user PC initiates the PPP connection and accesses the broadband network in the ADSL mode.
- In Figure 6-5, the IAD108 initiates the PPP connection and accesses the broadband network in the ADSL mode.

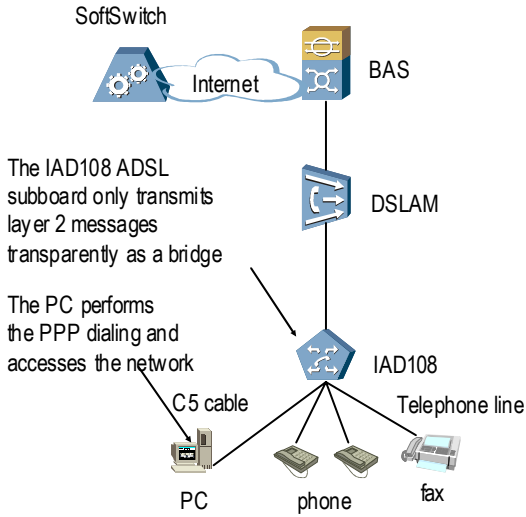


Figure 6-4 Networking of the user PC initiating the PPP connection in the bridging mode

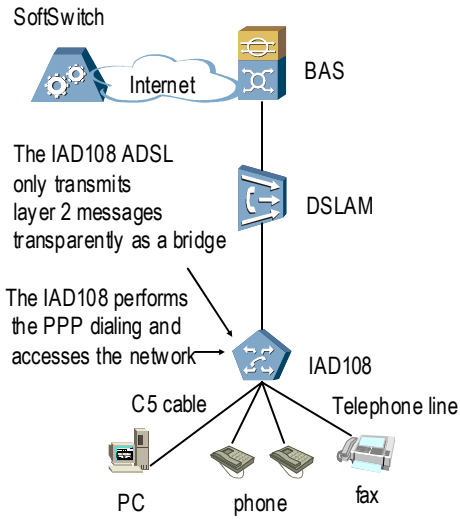


Figure 6-5 Networking of the IAD108 initiating the PPP connection in the bridging mode

6.3.3 Configuration Procedures

The configuration of ADSL services in the bridging mode includes four procedures as follows.

1) Setting the ATM attribute

- In the bridging mode or non-bridging mode, you must create an ATM interface and configure the VPI/VCI, to connect the uplink DSLAM equipment.
- The VPI/VCI value of the ADSL subboard is set to 0/35 by default. It must correspond with the setting of the uplink DSLAM. You can modify it with actual conditions.
- The ATM attribute is set first, and can be referenced or indirectly referenced by subsequent configurations. When

deleting the ATM attribute, make sure that subsequent configurations no longer reference or indirectly reference it. Otherwise, you cannot delete the ATM attribute.

Note:

Before configuring the ATM attribute, query if it has been configured. If yes, do not configure it again.

---

2) Checking the PPP interface

The PPP interface cannot exist in the bridging mode. You can use commands to query it. If it exists, delete it. If not, go on to configure the EoA interface.

3) Setting the EoA interface

The created EoA interface must be associated with the above ATM attribute. It encapsulates Ethernet data frames to ATM cells.

4) Setting the bridging port

Create the bridge that transmits layer 2 messages transparently. The bridge must be associated with the above EoA interface.

6.3.4 Configuration Examples

The configuration of the ADSL subboard in the bridging mode is as shown below.

1) Query if the ATM interface has been configured. If the interface exists, do not create again. Proceed as follows:

```
IAD2000(diagnose)%%adsl get ATM interface
```

```
{ <cr>|command<S><1,63> }:

Command:
                    adsl get ATM interface
get ATM interface
Error: No entry found
$
IAD2000(diagnose)%%
```

2) According to the above results, no ATM interface has been configured. Therefore, create an ATM interface with the name of “atm-0”. At most, you can configure eight PVCs. Proceed as follows:

```
IAD2000(diagnose)%%adsl create ATM interface ifname atm-0
maxvc 8
{ <cr>|command<S><1,63> }:

Command:
                    adsl create ATM interface ifname atm-0
maxvc 8
create ATM interface ifname atm-0 maxvc 8


Entry Created

I-Name         : atm-0       MaxVccs          : 8
CBRPriority    : 5            UBRPriority     : 1
RTVBRPriorit   : 4           NRTVBRPriority   : 3
GFRPriority    : 2           Latency         : Interleaved
```

```
MaxConfVccs     : 0
OAMSrc          : 0xffffffffffffffffffffffffffffffff
Oper Status     : Down        Admin Status    : Up
$
IAD2000(diagnose)%%
```

3) After creating the ATM interface, create a VC interface. The interface must be associated with the above "atm-0" at the bottom layer. Simultaneously, set the VPI/VCI to 0/35. Proceed as follows:

```
IAD2000(diagnose)%%adsl create atm vc intf ifname aal5-0
vpi 0 vci 35 lowif atm-0
{ <cr>|command<S><1,63> }:

Command:
                    adsl create atm vc intf ifname aal5-0
vpi 0 vci 35 lowif atm-0
create atm vc intf ifname aal5-0 vpi 0 vci 35 lowif atm-0



Entry Created



LowIf           : atm-0      VPI      : 0          VCI      :
35
VC IfName        : aal5-0      VC Type          : PVC
Admin Status     : Up          Oper Status      : Down
Aal5 Tx Size     : 9188         Aal5 Rx Size     : 9188
AAL Type         : AAL5        AAL5 Encap       : LLC Mux
```

```
Max Aal5 Proto  : 2           Trf Descr Index : 0
VC Weight       : 10          Creator         : nonilmi
$
IAD2000(diagnose)%%
```

4) If the VPI/VCI configured in the above VC needs to be modified, for example, to 1/32, use commands. During modification, specify that the VC interface “aa15-0” is associated with the VPI/VCI. Proceed as follows:

```
IAD2000(diagnose)%%adsl modify atm vc intf ifname aal5-0
vpi 1 vci 32
{ <cr>|command<S><1,63> }:

Command:
                    adsl modify atm vc intf ifname aal5-0
vpi 1 vci 32
modify atm vc intf ifname aal5-0 vpi 1 vci 32



Set Done



LowIf          : atm-0      VPI     : 1          VCI     :
32
VC IfName       : aal5-0      VC Type         : PVC
Admin Status    : Up          Oper Status     : Down
Aal5 Tx Size    : 9188        Aal5 Rx Size    : 9188
AAL Type        : AAL5        AAL Encap      : LLC Mux
```

```
Max Aal5 Proto  : 2           Trf Descr Index : 0
VC Weight       : 10          Creator         : nonilmi
$
IAD2000(diagnose)%%
```

5) Create an EoA interface with the name of “eoa-0”, and then specify that the port is associated with the VC interface “aa15-0” at the bottom layer. Proceed as follows:

```
IAD2000(diagnose)%%adsl create eoa intf ifname eoa-0 lowif
aal5-0
{ <cr>|command<S><1,63> }:

Command:
                    adsl create eoa intf ifname eoa-0 lowif
aal5-0
create eoa intf ifname eoa-0 lowif aal5-0



Entry Create



IfName              : eoa-0          Interface Sec Type:
Public
Configured IP Address: 0.0.0.0        Mask             :
0..0.0
Low IfName          : aal5-0         NAT Direction    :
OUT
Gateway             : 0.0.0.0        DRoute           :
```

```
False
Oper Status           Down            Admin Status      :
Up
UseDHCP              : False
$
IAD2000(diagnose)%%
```

6) Specify that the created EoA interface “eoa-0” is the bridging port. Proceed as follows:

```
IAD2000(diagnose)%%adsl create bridge port intf ifname
eoa-0
{ <cr>|command<S><1,63> }:

Command:
                  adsl create bridge port intf ifname
eoa-0
create bridge port intf ifname eoa-0


Entry Created


Port  If-Name  Delay-Exceed-Discards  MTU-Exceed-Discards
------------------------------------------------------
40       eoa-0     0                         0
$
IAD2000(diagnose)%%
```

7) Confirm the modification. Otherwise, the configuration will be lost after restart. Proceed as follows.

```
IAD2000(diagnose)%%adsl commit
{ <cr>|command<S><1,63> }:

Command:
                    adsl commit

IAD2000(diagnose)%%
```

The data configuration of the ADSL subboard connecting the DSLAM in the bridging mode is completed.

- For the network access of the user PC, configure the PPP account and password of the PC on the BAS equipment, and install the PPP software for dialing on the PC.
- For the network access of the IAD108, configure the PPP account and password of the IAD108 on the BAS equipment, and configure the PPP account and password on the IAD108.

Note:

If you are not familiar with the above command lines of the ADSL subboard, or need to configure more parameters, add "**help**" at the end of command words for help.

Chapter 7 Maintaining System

To ensure normal operation of the IAD108, you should carry out routine maintenance after the data has been configured correctly.

This chapter introduces the following maintenance operations:

- System management
- Access service management
- Management of operators
- Management of operation log
- Alarm management
- Common network tool

7.1 System Management

7.1.1 Saving Data

To ensure the system availability and data security, the IAD108 supports the saving of data. The configured system data is temporarily stored in the SDRAM. To prevent loss of data caused by unexpected events, you should save the configured data into the Flash memory.

The operations for saving data are as follows:

1) Query current data saving condition

Use command **show data unsaved percent** to display the percentage of unsaved configuration data.

```
IAD2000>show data unsaved percent
```

```
------------------------------------------------
  Now, the percentage of unsaved configuration data is:
25%
------------------------------------------------
IAD2000>
```

If some new data is configured, you can save the data directly.

2) Manually save the data

If there exists any unsaved data, you can carry out command **write** in privilege mode to save it.

Note:

No matter whether auto-saving is set, you can carry out command **write** to save the system configuration data.

7.1.2 Rebooting the System

In the privilege mode, you can run the command **reboot** to reboot the system.

IAD2000#**reboot**

The config data has been changed, config will be lost if reboot, continue? [Y|N]:**y**

Are you sure to reset system? [Y|N]:**y**

After executing the rebooting command, the system will display some prompt information. If you are sure to reboot the system, you can input “Y”.

⚠ **Caution:**

Rebooting the system will affect the currently running services, please use it cautiously.

7.1.3 Showing CPU Occupancy

In user mode, you can use command **show cpu** to show the CPU occupancy.

- When the occupancy exceeds 85%, the system will generate a CPU overload alarm.
- When the occupancy is lower than 75%, the alarm will be recovered.

Example:

```
IAD2000>show cpu
  CPU occupancy: 47%
IAD2000>
```

7.1.4 Showing System Date and Time

In user mode, you can use the command **show clock** to query the system time of IAD108, making sure that the time is accurate.

When you find that the system time of IAD108 is inaccurate, you can enter the privilege mode, use the **clock set** command to set system time. The format of time is set to be: **time** hh:mm:ss **date** yyyy-mm-dd.

Example:

Show the current time of system.

```
IAD2000>show clock
-------------------------------------------------
  System startup date: 2004-08-13 time: 09:55:30
  Current date: 2004-08-16
  Current time: 17:10:18
-------------------------------------------------
IAD2000>
```

Modify the system time to 2004-08-16, 17:10:00.

```
IAD2000#clock set 17:10:00 2004-08-16
  Current date: 2004-08-16
  Current time: 17:10:00
IAD2000#
```

7.1.5 Showing Version Information

I. Showing Version of IAD108 System

In user mode, you can run the command **show version** to display the versions of the Basic Input Output System (BIOS) and the system software.

Example: Show system version.

```
IAD2000>show version
  Equipment type            : IAD108
  Main Board PCB version    : AG21CSPA VER.A
  Software version          : IAD2000V200R002B01D031
  BIOS version              : 506
  SLIC version              : (U35-U38)015
  CPLD version              : (U16)100
  DSP version               : (U34)V100R1C1B23D10
IAD2000>
```

II. Showing MGCP Version

In user mode, you can use the command **show mgcp ver** to see the MGCP version.

Example:

```
IAD2000>show mgcp ver
MGCP version:  1
IAD2000>
```

7.1.6 Controlling the Information Output to the Terminals

The management of terminal information output includes setting terminal information output switch and information output level.

The terminal information of IAD108 include: system log (syslog), operation log (oprlog), debugging information (debug), alarm information (alarm), tracing information (trace), diagnosis information (diagnose), statistics information (stat) and other information (other).

The management and maintenance terminals of IAD108 include: command line terminal, Network Management Station (NMS), Web-based NMS and Log host.

Information generated on the IAD108 is not sent to the various terminals directly. Instead, it is first sent to the IAD108 information center. This information center controls the output of information to the various terminals, like which type of information, and what level of the information, should a terminal receive.

I. Setting Information Output Switch

By setting the information output switch, you can control the type of information to be outputted to a certain terminal.

1) Related commands

Table 7-1 Related commands

Operation	Command
Set the information output switch for command line	IAD2000(config)**#infoswitch cli**
Set the information output switch for NMS	IAD2000(config)**#infoswitch nms**
Set the information output switch for Log host	IAD2000(config)**#infoswitch syslog**
Set the information output switch for Web-based NMS	IAD2000(config)**#infoswitch www**
Show the information output switch for the command line	IAD2000>**show infoswitch cli**
Show the information output switch for the NMS	IAD2000>**show infoswitch nms**

Operation	Command
Show the information output switch for the log host	IAD2000>**show infoswitch syslog**
Show the information output switch for the Web-based NMS	IAD2000>**show infoswitch www**

2) Descriptions of commands:

- When you set the command line terminal information output switch and level, you should input the parameter "Client ID", which can be obtained through command **show client**. The **show client** command will display the information of command line client end of the registered users, including terminal user number (Client ID), user name, IP address and login time.
- You can set the output switch of multiple information types at the same time.

There are two switches controlling the report of alarm information to the command line terminal.

- Switch 1: Use the command **infoswitch cli** to set whether to report alarm information to the command line terminal. It controls the output of all the alarm information.
- Switch 2: Use the command (**no**) **alarm output** to set whether to send the corresponding alarm to the command line terminal according to a certain condition. It controls the alarm information according to the categories.

3) Usage example

Set not to send the system log to NMS SZ-CNC-WS_1, and send the alarm information, debugging information, diagnosis information to the command line terminal named “bbb”:

```
IAD2000(config)#infoswitch nms SZ_CNC_WS_1 syslog off
{  <cr>|oprlog<K>|debug<K>|alarm<K>|diagnose<K>|trace<K
>|stat<K>|other<K> }:

Command:
                infoswitch nms SZ_CNC_WS_1 syslog off
IAD2000(config)#disable
IAD2000>show client

-----------------------------------------------------
-
  Client ID    Client Name    IP Address    Login Time

-----------------------------------------------------
-
   1     root     0.  0.  0.  0     2004-08-17 10:37:48
   2     aaa    172. 21. 50.  8     2004-08-17 10:41:05
   3     bbb    172. 21. 50. 13     2004-08-17 10:41:37
   4     ccc    172. 21. 50.  6     2004-08-17 10:41:58

-----------------------------------------------------
-
IAD2000>
```

According to the *Client Name,* you can get the *Client ID* of user "bbb", which is 3. Then set the information output switch according to the *Client ID.*

```
IAD2000(config)#infoswitch cli 3 alarm on debug on
diagnose on
{ <cr>|syslog<K>|oprlog<K>|trace<K>|stat<K>|other<K> }:

Command:
                infoswitch cli 3 alarm on debug on
diagnose on
IAD2000(config)#
```

Note:

Operator who maintains the system through the serial port has a fixed Client ID of 1, and the IP address displays as 0.0.0.0.

II. Setting Information Output Level

By setting the information output switch, you can control the level of information to be outputted to a certain terminal.

Table 7-2 Related commands

Operation	Command
Set the information output level for command line	IAD2000(config)**#infolevel cli**
Set the information output level for NMS	IAD2000(config)**#infolevel nms**
Set the information output level for log host	IAD2000(config)**#infolevel syslog**

Operation	Command
Set the information output level for Web-based NMS	IAD2000(config)#**infolevel www**
Show the information output level for the command line	IAD2000>**show infoswitch cli**
Show the information output level for the NMS	IAD2000>**show infolevel nms**
Show the information output level for the Log host	IAD2000>**show infolevel syslog**
Show the information output level for the Web-based NMS	IAD2000>**show infolevel www**

1) Descriptions of commands

- To set information output level, first turn on the information output switch, and then control the output level of the information.
- The higher the level is, the more important the information is.
- Once a level is set, other information with a higher level will be outputted to the specified terminal.
- The default output level is 0, which means all the information will be exported.
- You can set in one time the level of multiple types of information to be outputted to the same terminal.

2) Usage example

Set the output level of syslog to NMS SZ-CNC-WS_1 as 3, and set the output levels of alarm, debugging and diagnosis information to command line terminal with Client ID 3 to 1, 2 and 3 respectively.

```
IAD2000(config)#infolevel nms SZ_CNC_WS_1 syslog 3
{  <cr>|oprlog<K>|debug<K>|alarm<K>|diagnose<K>|trace<K
>|stat<K>|other<K> }:

Command:
                infolevel nms SZ_CNC_WS_1 syslog 3
IAD2000(config)#infolevel cli 3 alarm 1 debug 2 diagnose
3
{ <cr>|syslog<K>|oprlog<K>|trace<K>|stat<K>|other<K> }:

Command:
                infolevel cli 3 alarm 1 debug 2 diagnose
3
IAD2000(config)#
```

7.2 Access Service Management

7.2.1 Starting/Terminating Access Service

I. Ordinary Access Service

The IAD108 can start or terminate the service, in order to facilitate the management on the online accessed subscribers. The related commands are listed below.

Table 7-3 Related commands

Operation	Command
Terminate service forcibly	IAD2000#**endservice** *portid*
Restart service	IAD2000#**startservice** *portid*

portid: Number of the port, of which the service is to be terminated. The value ranges from 0 to 7.

II. SPC Service

The start or termination of Semi-Permanent Connection (SPC) service is actually the linking or releasing of the SPC. After you have released an SPC, the relevant configuration data is not removed. You can establish the SPC again when necessary.

Table 7-4 Related commands

Operation	Command
Release an SPC	IAD2000(config)#**spc release** { **connectid** *connectid* | **from-connectid** *fromid* [**to-connectid** *endid*] }
Recover an SPC	IAD2000(config)# **no spc release** { **connectid** *connectid*| **from-connectid** *fromid* [**to-connectid** *endid*] }

The parameters of the commands are listed in Table 7-5.

Table 7-5 Parameters of the commands related to SPC services

Item	Description
connectid	Index of SPC, ranging 0–7.
fromid	Index of the start SPC, ranging 0–7.
endid	Index of the end SPC, ranging 0–7.

7.2.2 Resetting Access User Port

In glob config mode, you can execute command **reset** *portid* to reset the access user port.

Caution:

If you reset the access user port, the established services will be interrupted. Use it cautiously.

7.2.3 Showing Port Status

In the user mode, you can run the command **show port state** [*portid*] to display the port status information.

portid: Number of the port, ranging 0–7. If no port number is entered, the status of all the ports will be shown.

Example: Show the status of No.6 port.

```
IAD2000>show port state 6

------------------------------------------------------
-
   Port  PortType State    ServiceType   ServiceState

------------------------------------------------------
-
```

```
        6   PSTN    Idle    Instant service   Start service

-------------------------------------------------------
-
IAD2000>
```

7.2.4 Showing Access User Data

I. Ordinary Access User

In the user mode, you can run the command **show mguser** [*portid*] to display the service data of the access users.

Example: Show the user data of No.5 port.

```
IAD2000>show mguser 5
-------------------------------------------------------
-
   Port MGID TerminalID Priority LWDflag Telno MGtelno

-------------------------------------------------------
-
   5     0           5       Low       No             -
-

-------------------------------------------------------
-
IAD2000>
```

II. SPC User

In user mode, you can use the command **show spc** [**connectid** *connectid* | **from-connectid** *fromid* [**to-connectid** *endid*]] to query the SPC data.

Example: Show SPC users.

```
IAD2000>show spc
{ <cr>|connectid<K>|from-connectid<K> }:

Command:
        show spc

-----------------------------------------------------
-
  index   state   type   Port  Port  name
  0       Normal  IP-SPC   1   -    ipspc
IAD2000>
```

7.2.5 Sending On-hook Signals to Console

After an IAD subscriber hooks on, the IAD can be configured to send the on-hook signals to the IP console, so as to facilitate the console to charge accurately.

Table 7-6 Related commands

Operation	Command
Send on-hook signal to IP console	IAD2000(config)#**console** *ip*
Cancel the sending of on-hook signal to IP console	IAD2000(config)#**no console**

The parameter *ip* is the IP address of the console.

Example:

Configure the IAD to send the on-hook signals to the IP console, of which the IP address is 192.20.129.2.

```
IAD2000(config)#console 192.20.129.2
IAD2000(config)#
```

7.3 Operator Management

Operators here refer to those people who maintain and operate on the IAD108 through the command line terminal. It accepts user login only through the matching of user name and password. In addition, by dividing the authorities of operators into several levels, IAD108 can control the operators for specific maintenance to the equipment. IAD108 is strict to the identification check of operators.

Table 7-7 Task list for managing operators

Serial No.	Operation	Command
1	Add/delete an operator	IAD2000(config)# (**no**) **user name**
2	Set operator authority	IAD2000(config)#**user level**
3	Change operator password	IAD2000(config)#**user password**
4	Set reenter number for the operator	IAD2000(config)#**user reenter**
5	Set operator's Appendix information	IAD2000(config)#**user apdinfo**

Serial No.	Operation	Command
6	Show operator information	IAD2000>**show terminal user**{ *username* | **all** | **online** } IAD2000>**show client**
7	Disconnect an operator	IAD2000#**user disconnect** *clientid*

7.3.1 Adding/Deleting Operator

I. Adding Operators

Each operator has a unique user name. By default, the system provides one super administrator, with user name as “root” and password as “admin”. The requirements on user name and password are as follows.

User name: It consists of 1–15 printable characters (without spaces in between). There mustn’t exist two identical names.

Password: It can be set by the user, containing 1–15 characters. It must be correctly inputted when logging in.

When an operator logs in, and the user name matches the password, the system will check whether the user name is in use. If the user name has been registered on the Console, the system will decide whether to accept or reject the login request according to the configured number for allowed users.

You can add multiple operators at one time, and at most 126 operators can be added to the system.

Example: Add a user, with user name and password both as "user1", authority as ordinary user, and reenter times as 3.

```
IAD2000(config)#user name
  User Name(<=15 chars):user1
  User Password(<=15 chars):
  Confirm Password(<=15 chars):
  User's Level(1--3).
     1.Exec      2.Oper    3.Admin:1
  Permitted Reenter Number(0--4):3
  Language(0.local, 1.general):1
  This user is added!
  Continue? [Y|N]:n
IAD2000(config)#
```

Note:

Here, "Continue" means to ask the user whether continue to add operators.

II. Deleting Operators

When deleting an operator, you should pay attention to the following:

- An operator cannot delete himself/herself.
- An operator who is logging in cannot be deleted. If you really need to delete this operator, you should first disconnect this operator.

- An operator with higher authority can use the command **user disconnect** to reject a logging in Telnet operator who has a lower authority.
- You can delete multiple operators in one time.

Example: Delete the operator “aaa”:

```
IAD2000(config)#no user name
  User Name(<=15 chars):aaa
  This user is deleted!
  Continue? [Y|N]:n
IAD2000(config)#
```

7.3.2 Setting Operator Authority

Generally, the authority of an operator has already been set when the operator was added to the system. If the authority of a certain operator should be changed, an Admin can do the job. The authority control among users with different authority levels are as follows.

- The super administrator “root” can change the authorities of all the operators.
- Admin operators can change the authorities of the Oper operators and Exec operators, but cannot change that of himself or other Admin operators.
- Oper operators and Exec operators cannot change the authorities of themselves.

Example: Change the authority of operator “aaa” from Exec to Oper.

```
IAD2000(config)#user level
  User Name(<=15 chars):aaa
```

```
      1.Exec      2.Oper    3.Admin:
    User's Level(1--3).2
    Confirm Level(1--3): 2
    Changed ok!
    Continue? [Y|N]:n
IAD2000(config)#
```

7.3.3 Changing Operator's Password

The users with different authorities can modify their passwords by following the rules below.

- Operators of Root and Admin level can directly change their own and others' login passwords, by executing command **user password**.
- Operators of Admin level can not modify the passwords of other Admin operators. An Oper operator can only change his/her own password, and the original password must be inputted when changing the password.
- An Exec operator cannot change his/her own password.

Example: Change the password of Admin operator "bbb".

```
IAD2000(config)# user password
User Name(<=15chars): bbb
New Password(<=15chars):
Confirm Password(<=15 chars):
Changed ok!
Continue?[Y|N] n
```

7.3.4 Setting Reenter Number

The reenter number of an operator is generally set as 1 when the operator is added into the system. If the reenter number of a certain operator should be changed, the Root or Admin can do the job.

The users with different authorities can modify their reenter times by following the rules below.

- Root can change the reenter numbers of all the operators.
- Admin operator can change the reenter numbers of Oper operators and Exec operators, but cannot change that of other Admin operators.
- Oper operators and Exec operators cannot change the reenter numbers of themselves and others.

Note:

The reenter number of an operator ranges from 0 to 4. When it is 0, the operator cannot log in to the system.

Example: Modify the reenter number of user “bbb” to 2:

```
IAD2000(config)#user reenter
  User Name(<=15 chars):bbb
  Permitted Reenter Number(0--4):2
  Confirm Reenter Number(0--4):2
  Changed ok!
  Continue? [Y|N]:n
```

```
IAD2000(config)#
```

7.3.5 Setting Operator's Appendix Information

The operator appendix information is an appendix on the operator, which can be the contact methods and address of the operator.

The users with different authorities can modify their appendix information by following the rules below.

- Root and Admin operators can change the appendix information of all the operators that have a lower authority.
- Oper operators can only change the appendix information of themselves.
- Exec operators cannot change their own appendix information.

Example: Root sets the appendix information of operator "Huawei" as "phone 0755-26540808":

```
IAD2000(config)# user apdinfo
  User Name(<=15 chars):huawei
  User Append Info: 0755-28780808
  Changed ok!
  Continue? [Y|N]:n
IAD2000(config)#
```

7.3.6 Showing Operator's Information

I. Show Terminal User

To manage an operator, such as modify the attributes of the operator, you may need to know the information about all the operators or an individual operator.

- Command **show terminal user** *username* can be used to display the information of an operator.

Command **show terminal user all** can be used display the information of all the operators.

- Command **show terminal user online** to display the information of all the online operators.

Example: Show the information of all operators.

```
IAD2000(config)#show terminal user all
  -----------------------------------------------------
  Name           Level    Status  ReEnterNUM AppendInfo
  -----------------------------------------------------
  system         ADMIN    OFFLINE 1
  root           SUPER    ONLINE  1
  user1          USER     OFFLINE 3
  aaa            OPERATOR ONLINE  1
  bbb            USER     ONLINE  2
  huawei        USER    ONLINE  1         0755-28780808
  -----------------------------------------------------
IAD2000(config)#
```

II. Showing Client

Sometimes you may need to know from which terminal an operator has logged in, the IP address of the terminal, and the Client ID. In this case, you can run the command **show client**.

Example: Show the information of login operator:

```
IAD2000> show client
-----------------------------------------------------
-
  Client ID     Client Name     IP Address     Login Time

-----------------------------------------------------
-
   1     root      0.  0.  0.  0     2004-08-17 11:58:45
   2    huawei     172. 21. 50. 8     2004-08-17 12:21:45
   3     aaa      172. 21. 50. 13     2004-08-17 12:21:52
   4     bbb      172. 21. 50. 6     2004-08-17 12:22:06

-----------------------------------------------------
-
IAD2000(config)#
```

Note:

Operators who maintain the system through the serial port have a fixed Client ID of 1, and the IP address displays as 0.0.0.0.

7.3.7 Disconnecting Login Operator

You can use the command **user disconnect** *clientid* to disconnect an operator who logs in through a Telnet connection. When using this command, you should input the Client ID, which can be obtained through the command **show client**.

Example: Disconnect the user logged in from 10.11.136.23 (its Client ID is queried to be 3):

```
IAD2000# user disconnect 3
Success Operation
IAD2000(config)#
```

Note:

Using command **user disconnect**, you can only disconnect the operators who have logged in the system through Telnet connection, rather than the operators who have logged in the system through serial port.

7.4 Management of Operation Log

IAD108 provides log function, recording the operation and maintenance information of the system, including the remote maintenance information.

IAD108 can record the latest 512 pieces of operation logs, and some of the important information can be recorded on the internal loghost through Syslog mechanism.

To implement log function, you should assign the IP address of the log host on the IAD108, and make necessary configuration on the corresponding log host.

Table 7-8 Related commands

Operation	Command
Add a log host	IAD2000(config)**loghost add**
Delete a log host	IAD2000(config)**loghost delete**
Activate the log host	IAD2000(config)**loghost active**
Deactivate the log host	IAD2000(config)**no loghost active**
Show the operation log by serial No.	IAD2000>**show log detailed**
Show log list	IAD2000>**show log list**
Show configuration information of log host	IAD2000>**show loghost list**
Set information output control switch of log host	IAD2000(config)**infoswitch syslog**
Set information output control level of log host	IAD2000(config)**infolevel syslog**
Query information output control switch of log host	IAD2000>**show infoswitch syslog**
Query information output control level of log host	IAD2000>**show infolevel syslog**

7.4.1 Adding Log host

I. Command Description

The log host is used to receive log information generated by the system. The parameter of the log host must be added in IAD108 before the log host is used; otherwise the system will not send the log to the host, and the user can not query the log in log host.

In global config mode you can execute command **loghost add** *ip hostname* to add the log host.

Example: Add a log host "log", with IP address as 210.11.123.56.

```
IAD2000(config)# loghost add 210.11.123.56 log
IAD2000(config)#
```

II. Parameter Descriptions

ip: IP address of the log host, which is in dotted decimal notation.

hostname: Name of the log host, a string of no more than 31 characters. It cannot be null.

Note:

- There can be no repeated log host name or IP address.
- When a log host is added, it will not receive log information reported from the system until the log host is activated.

7.4.2 Deleting Log Host

In global config mode, you can execute command **loghost delete** { *ip* | *hostname*} to delete the log host.

Example: Delete the log host whose IP address is 210.11.123.56.

```
IAD2000(config)# loghost delete 210.11.123.56
IAD2000(config)#
```

Note:

- To delete a log host, you can delete it by its IP address or its host name.
- A log host in any mode can be deleted.
- Delete the log host if its IP address is changed or it is no longer used.

7.4.3 Activating Log Host

In global config mode, you can use the command **loghost active** { *ip* | *hostname* } to activate the log host.

Example: Activate the log host “log”, whose IP address is 210.11.123.56.

Activate it by IP address:

```
IAD2000(config)#show loghost list
{ <cr>|ip<I>|hostname<S><1,31> }:

Command:
```

```
                show loghost list
-----------------------------------------------------
-

  IP ADDRESS          HOSTNAME          TERMINAL STATUS
  210.11.123.56       log               DEACTIVE

-------------------------------------------------


IAD2000(config)#loghost active 210.11.123.56
IAD2000(config)#show loghost list
{ <cr>|ip<I>|hostname<S><1,31> }:
Command:
                show loghost list
-----------------------------------------------------
-

  IP ADDRESS          HOSTNAME          TERMINAL STATUS
  210.11.123.56       log               NORMAL
-----------------------------------------------------
-


IAD2000(config)#
```

Activate the loghost “log” by host name:

```
IAD2000(config)#show loghost list
{ <cr>|ip<I>|hostname<S><1,31> }:

Command:
                show loghost list
```

```
-----------------------------------------------------
-

  IP ADDRESS          HOSTNAME          TERMINAL STATUS
  210.11.123.56       log               DEACTIVE
-----------------------------------------------------
-


IAD2000(config)#loghost active log
IAD2000(config)#show loghost list
{ <cr>|ip<I>|hostname<S><1,31> }:

Command:
                show loghost list
-----------------------------------------------------
-

  IP ADDRESS          HOSTNAME          TERMINAL STATUS
  210.11.123.56       log               NORMAL
-----------------------------------------------------
-

IAD2000(config)#
```

Note:

- When a log host is added, it will not receive log information reported from the system until the log host is activated.
- A log host can be activated by its IP address or its host name.

7.4.4 Deactivating Log Host

In global config mode, you can use the command **no loghost active** { *ip* | *hostname* } to deactivate the log host

Example: Deactivate the log host “log”, whose IP address is 210.11.123.56.

Deactivate the log host “log” by IP address:

```
IAD2000(config)#show loghost list
{ <cr>|ip<I>|hostname<S><1,31> }:

Command:
                show loghost list
-------------------------------------------------------
-

  IP ADDRESS          HOSTNAME          TERMINAL STATUS
  210.11.123.56       log               NORMAL
-------------------------------------------------------
-

IAD2000(config)#no loghost active 210.11.123.56
```

```
IAD2000(config)#show loghost list
{ <cr>|ip<I>|hostname<S><1,31> }:

Command:
                show loghost list
-------------------------------------------------------
-

  IP ADDRESS          HOSTNAME          TERMINAL STATUS
  210.11.123.56       log               DEACTIVE
-------------------------------------------------------
-

IAD2000(config)#
```

Deactivate the log host “log” by host name:

```
IAD2000(config)#show loghost list
{ <cr>|ip<I>|hostname<S><1,31> }:

Command:
                show loghost list
-------------------------------------------------------
-

  IP ADDRESS          HOSTNAME          TERMINAL STATUS
  210.11.123.56       log               NORMAL
-------------------------------------------------------
-
```

```
IAD2000(config)#no loghost active log
IAD2000(config)#show loghost list
{ <cr>|ip<I>|hostname<S><1,31> }:

Command:
                show loghost list
-------------------------------------------------------
-

  IP ADDRESS          HOSTNAME          TERMINAL STATUS
  210.11.123.56       log               DEACTIVE
-------------------------------------------------------
-

IAD2000(config)#
```

Note:

- A log host can be activated by its IP address or its host name.
- For the log host that is temporarily not in use, deactivate it.

7.4.5 Showing Operation Log Information

I. Command Description

In user mode, the Oper operator can use the command **show log detailed** *index1* [*index2*] to display log information by serial No.

Example: Show the detailed information of logs numbering from 1 to 10:

```
IAD2000>show log detailed 1 10
         1  enable
         2  configure terminal
         3  user name
         4  no user name
         5  user name
         6  write
         7  enable
         8  enable
         9  enable
        10  enable
 ---------
IAD2000>
```

II. Parameter Description

index1: The start index number of the log to be queried

index2: The end index number of the queried log, which cannot be smaller than *index1*.

7.4.6 Showing Operation Log List

I. Command Description

In the user mode, an Exec operator can perform the following operations:

- Runs the command **show log list** *username* [*date*] to show the log list of a certain operator.
- Run the command **show log list all** [*date*] to display the log lists of all the operators.

You can query the log records according to specific operator, or according to time segment. If you do not specify the time segment, all the records will be shown.

Through this command, the configuration made on the device through command line terminal can be queried. Meanwhile, you can also see what kind of configurations have been made on the device by which operator. If any user is found to be doing illegal configurations or is harming the equipment, their operation authorities are to be degraded or canceled.

Note:

For operation commands that are relatively long, if you use command **show log list** to query, only the several characters in the front part are displayed with "..." as abbreviation. If detailed information is needed to be shown, you can use the command **show log detailed**.

Example: Show the operation log of user "root"

```
IAD2000>show log list root
{ <cr>|date<D><yyyy-mm-dd> }:

Command:
```

```
        show log list root
 No. UserName Command          Data&Time         LogMode
IPAdd
1    root   enable          08/17/2004 14:54:14 Terminal
0.0.0.0
2      root     configure terminal   08/17/2004 14:54:15
Terminal 0.0.0.0
3    root   user name        08/17/2004 14:56:34 Terminal
0.0.0.0
4    root   no user name     08/17/2004 14:57:09 Terminal
0.0.0.0
5    root   write           08/17/2004 14:58:30 Terminal
0.0.0.0
IAD2000>
```

II. Parameter Descriptions

all: Display the operation log information of all users.

username: User name. It is used to display log information of a specified user.

date: The time segment of logs to be shown. Only logs within the time segment will be displayed.

7.4.7 Showing Log Host Configurations

I. Command Description

In user mode, Oper operators can use the command **show loghost list** [*ip* | *hostname*] to query the configuration information of log host, including IP address, host name, state (activated or not).

Note:

- Log host information can be shown by its IP address or host name.
- If no host is specified, all log host information will be displayed.

Example: Show the information of all log hosts.

```
IAD2000>show loghost list
{ <cr>|ip<I>|hostname<S><1,31> }:

Command:
        show loghost list
-------------------------------------------------------
-

  IP ADDRESS          HOSTNAME          TERMINAL STATUS
  210.11.123.56       SZ_CNC_WS_1       DEACTIVE
  172.21.50.51        log               NORMAL
-------------------------------------------------------
-
```

```
IAD2000>
```

II. Parameter Descriptions

ip: IP address of log host.

hostname: Name of log host.

7.4.8 Setting Information Output Control Switch of Log Host

I. Command Description

Only when the related information switch is set to “on”, can the information be sent to the related log host. For detailed descriptions of information output control switch, please refer to section 6.1.6.

In global config mode, you can execute the following command to set the switch for controlling the output of log host information.

infoswitch syslog {*ip* | *hostname*} **{syslog** *value* | **oprlog** *value* | **debug** *value* | **alarm** *value* | **trace** *value* | **diagnose** *value* | **stat** *value* | **other** *value*}

Note:

- This command is used to change the control switch for exporting log host information, which exists on the log host. When modifying, you can focus on a certain information type, or on multiple types.
- When executing this command, you must activate the related log host.

Example: Set the output control switches on log host “log2” as: only that for the (diagnose) terminal information type is set to “off”, others are set to “on".

```
IAD2000(config)#infoswitch syslog log2 alarm on debug on
diagnose off oprlog on other on stat on syslog on trace
on
IAD2000(config)#
```

II. Parameter Descriptions

The main parameters are listed in Table 7-9.

Table 7-9 Parameter descriptions

Item	Description
ip	IP address of log host
hostname	Name of log host
syslog	System log (info type)
oprlog	Operation log (info type)
debug	Debugging (info type)

Item	Description
alarm	Alarming (info type)
trace	Tracing (info type)
diagnose	Diagnosis (info type)
stat	Statistics (info type)
other	Other (info type)
value	Value of information switch, which can be set as “on” or “off”. “on” means allow the information output, “off” means not allow it.

7.4.9 Setting Information Output Control Level of Log Host

I. Command Description

In global config mode, the following command can be used to set the control level for exporting the information of existing log host.

infolevel syslog {*ip* | *hostname*} **{syslog** *value* | **oprlog** *value* | **debug** *value* | **alarm** *value* | **trace** *value* | **diagnose** *value* | **stat** *value* | **other** *value*}

Note:

- When setting the information output control level for a log host, such log host must be activated.
- Only when the switch of related information type is set to on, can the setting be effective.
- Only when the level of the information type to be outputted is higher than or equal to the preset value, can the information be allowed to be outputted to the corresponding log host.
- You can set the operation focusing on information types, and operate multiple information types simultaneously.

Example: Set all the information output control levels to log host "log" as 0:

```
IAD2000(config)#infolevel syslog log syslog 0 alarm 0
debug 0 diagnose 0 oprlog 0 other 0 stat 0 trace 0
IAD2000(config)#
```

II. Description of Principal Parameters

value: Information level value, ranging 0–4 (0 is the lowest level, and 4 is the highest level). Only when the level of the information type to be outputted is higher than or equal to the preset value, can the information be allowed to be sent to the corresponding log host.

7.4.10 Querying Information Output Control Switch of Log Host

In the user mode, run the following command to display the information output control switch of an existing log host.

show infoswitch syslog { *ip* | *hostname* } [**syslog** | **oprlog** | **debug** | **alarm** | **trace** | **diagnose** | **stat** | **other**] { *ip* | *hostname* }

Operations can be carried out on one or multiple information types. If information type is not specified, the information of all the information types will be displayed.

Example: Show the information output control switches for an existing log host “log”.

```
IAD2000>show infoswitch syslog 172.21.50.51 alarm debug
diagnose oprlog other stat syslog trace
  The terminal info output switch:
  SYSLOG_TYPE:on
  OPRLOG_TYPE:on
  DEBUG_TYPE :on
  ALARM_TYPE : 0-all; 1-no
  DIAG_TYPE  :on
  TRACE_TYPE :on
  STAT_TYPE  :on
  OTHER_TYPE :on
IAD2000>
```

7.4.11 Showing Information Output Control Level of Log Host

In the user mode, you can run the following command to show the information output control level of an existing log host.

show infolevel syslog [**syslog** | **oprlog** | **debug** | **alarm** | **trace** | **diagnose** | **stat** | **other**] { *ip* | *hostname* }

Note:

- Information level value, ranging 0–4 (0–4 are information levels, and 4 is the highest level).
- Operations can be carried out on one or multiple information types. If information type is not specified, the information of all the information types will be shown.

Example: Show the information output control levels of the alarm information type and other information types of the log host whose name is “log”.

```
IAD2000>show infolevel syslog log alarm debug diagnose
oprlog other stat syslog trace
 The terminal info output level:
  SYSLOG_TYPE:0
  OPRLOG_TYPE:0
  DEBUG_TYPE :0
  ALARM_TYPE : 0-all; 1-no
  DIAG_TYPE  :0
```

```
    TRACE_TYPE :0
    STAT_TYPE  :0
    OTHER_TYPE :0
IAD2000>
```

7.5 Alarm Management

Alarm management includes alarm record, alarm setting, alarm statistics of IAD108. IAD108 can be maintained through alarm management, so as to ensure its normal and efficient operation.

After an alarm is generated, the system will broadcast it to each terminal according to the conditions of the maintenance terminals currently configured, mainly including NMS terminal and command line terminal.

Whether to report the alarm to each terminal is defined in the alarm control.

7.5.1 Description of Common Alarm Attributes

1) Alarm ID

A certain type of alarms refers to all the alarms of the same type (with the same alarm ID). The alarm name corresponding to each alarm ID can be shown via the command **show alarm list**.

Note:

Alarms of the same type are identified by a unique alarm ID of four bytes, like 0x********. You can input the complete alarm ID like 0x********, or input it in decimal form. The value of an alarm ID ranges from 38 to 1507589.

2) Alarm level

Alarm level indicates the severity of an alarm, which can be critical, major, minor or warning.

- Critical alarm refers to the alarms for the faults which can affect the normal operation of the equipment, and the user is required to mend the faults immediately. Such as faults of power supply or circuits.
- Major alarm refers to board alarms or line alarms. If the user does not handle the fault in time, normal operation of services will be affected. Such as fault of a physical line.
- Minor alarm refers to the fault alarms and event alarms describing the working status of each board or line. For example, bit error occurs in a certain physical line.
- Warning alarm refers to a change of status, or an event, that does not affect the normal service of the device, but may be of interest to the maintenance and operation person. The recovery prompt of the device is also a warning.

3) Alarm class

There are three alarm classes:

- Event alarm

- Fault alarm
- Restore alarm

4) Alarm type

The alarms of IAD108 can be divided into five types:

- Communication alarm
- Service_quality alarm
- Process_error alarm
- Equipment alarm
- Environmental alarm.

5) Alarm parameter

It is a part of the alarm information, which is indicated in the reported alarm information description. The parameters for board alarms include frame number, slot number, and port number.

7.5.2 Alarm Management Task

The usually used alarm management tasks and commands are listed in Table 7-10.

Table 7-10 Alarm management task list

Operation	Command
Show alarm records	IAD2000>**show alarm record**
Show alarm configuration information	IAD2000>**show alarm content** *alarmid*
Set alarm output to command line terminal	IAD2000(config)#(**no**) **alarm output**

7.5.3 Showing Alarm Records

An alarm record includes the alarm generation time, serial number of the alarm, alarm level, alarm type, alarm class, alarm description, alarm parameters, etc.

IAD108 stores the alarm information in the host, and maintenance personnel can query it at any time.

IAD108 stores a maximum of 500 alarms currently generated. When a new alarm occurs, and if the record list is full, the old record will be replaced with the new one.

The specific operations are as follows:

I. Querying by Alarm Serial Number

Command: **show alarm record alarmsn** *sn*

It is the most direct method to query alarm record by alarm serial number. Because each alarm has its own serial number (generally, the alarms are numbered according to the alarm generation sequence), a certain alarm (the only one) can be directly located.

sn: Serial number of the alarm. It is a numerical value with the value range as [0, 4294967295].

II. Showing by Alarm ID

Command: **show alarm record alarmid** *id* [*startnum number*]

This method can be adopted when you want to query whether a certain alarm is generated. The meanings of the parameters in the command are listed in Table 7-11.

Table 7-11 Parameters of the command

Item	Description
id	Alarm ID, ranging 52–1572886.
startnum	The alarm number from which the display starts, the value range is 1–1000. In the Command Line Interface (CLI), you can start the display from 1, or from a designated *startnum*.
number	Maximum number of alarm records after the *startnum* that can be displayed in one time. It is an optional parameter, ranging 1–1000.

III. Querying by Alarm Level

Command: **show alarm record alarmlevel** *level* [*startnum number*]

This method can be adopted for showing alarm record if you only focus on alarms of a certain level. The meanings of the parameters in the command are listed in Table 7-12.

Table 7-12 Parameters of command

Item	Description
level	Alarm level. There are four levels. It is only necessary to input the English word indicating the corresponding level directly.

Item	Description
startnum	The alarm number from which the display starts, the value range is 1–1000. In the Command Line Interface (CLI), you can start the display from 1, or from a designated *startnum*.
number	Maximum number of alarm records after the *startnum* that can be displayed in one time. It is an optional parameter, ranging 1–1000.

IV. Querying by Alarm Type

show alarm record alarmtype *type_value* [*startnum number*]

You can use this command to query the alarms by alarm type.

The meanings of the parameters in the command are listed in Table 7-13.

Table 7-13 Parameters of command

Item	Description
type_value	Alarm type. There are five types: communication alarm, service_quality alarm, process_error alarm, equipment alarm and environmental alarm. It is only necessary to input the English word indicating the corresponding type directly.
startnum	The alarm number from which the display starts, the value range is 1–1000. In the Command Line Interface (CLI), you can start the display from 1, or from a designated *startnum*.
number	Maximum number of alarm records after the *startnum* that can be displayed in one time. It is an optional parameter, ranging 1–1000.

V. Query by Alarm Class

Command: **show alarm record alarmclass** *class* [*startnum number*]

You can use this command to query alarms by alarm class.

The meanings of the parameters in the command are listed in Table 7-14.

Table 7-14 Parameters of command

Item	Description
Class	Alarm class. There are three classes: event alarm, fault alarm and recovery alarm. It is only necessary to input the English word indicating the corresponding class directly.
startnum	The alarm number from which the display starts, the value range is 1–1000. In the Command Line Interface (CLI), you can start the display from 1, or from a designated *startnum*.
number	Maximum number of alarm records after the *startnum* that can be displayed in one time. It is an optional parameter, ranging 1–1000.

VI. Query by Alarm Generation Time

Command: **show alarm record alarmtime** *datebegin timebegin dateend timeend* [*startnum number*]

You can use this command to query the alarms generated within a certain time segment.

The meanings of the parameters in the command are listed in Table 7-15.

Table 7-15 Parameters of command

Item	Description
datebegin	Begin date. Input format: yyyy-mm-dd.
timebegin	Begin time. Input format: hh:mm:ss.
dateend	End date. Input format: yyyy-mm-dd.
timeend	End time. Input format: hh:mm:ss.
startnum	The alarm number from which the display starts, the value range is 1–1000. In the Command Line Interface (CLI), you can start the display from 1, or from a designated *startnum*.
number	Maximum number of alarm records after the *startnum* that can be displayed in one time. It is an optional parameter, ranging 1–1000.

VII. Querying Latest Alarms

Command: **show alarm record all**

You can use this command to query all the latest alarms conveniently.

Note:

The IAD108 stores 500 alarm records. If you need to query the alarms that occurred even earlier, you can find them in the database on the NMS.

7.5.4 Showing Alarm Configuration Information

In IAD108, an alarm has the following attributes: alarm ID, alarm name, alarm level, default alarm level, alarm type, alarm class, command line output flag, statistics flag, number of parameters, 15-minute threshold, 24-hour threshold, and detailed alarm explanation.

You can query the alarm attribute through the command below.

show alarm content *alarmid*

alarmid: Alarm ID

7.5.5 Setting Alarm Output to Command Line Terminal

After generated by the system, all the alarms will be reported to the command line terminal by default. However, due to different requirements and concerns by the users, IAD108 provides the alarm output mask function. You can set whether export the alarms to command line by alarm ID, alarm level, alarm type, and all alarms.

Note:

There are two switches controlling the report of alarm to the command line terminal. Switch 1: Use the command **infoswitch cli** to set whether to report alarm information to the command line terminal. Switch 2: Use the command (**no**) **alarm output** to set whether to send the corresponding alarm to the command line terminal by a certain condition. To sum up, switch 1 controls the output of all the alarm information, while switch 2 controls the output of information according to the alarm classes. Please refer to section 7.1.6 I. for the use of switch 1.

Each alarm has an output flag, which is used to identify whether the alarm should be outputted to command line, and the output setting command is also executed on the basis of this flag.

The basic command used for setting alarm output is:

(**no**) **alarm output**.

no is an optional item. **no alarm output** indicates the setting of not outputting a certain type of alarms to command line. **alarm output** indicates the setting of outputting a certain type of alarms to command line.

I. Setting by Alarm ID

Command: (**no**) **alarm output alarmid** *id*

Because alarm ID is unique for an alarm, this command will enable your to set clearly whether to output a certain type of alarms.

Description of principal parameter:

id: Alarm ID, ranging 52–1572886.

II. Setting by Alarm Level

Command line: (**no**) **alarm output alarmlevel** *level*

You may not concern about the alarms of lower level, and this command can be used to set not output all the alarms of a certain level.

level: Alarm level. There are four levels: critical alarm, major alarm, minor alarm and warning alarm. It is only necessary to input the English word indicating the corresponding level directly.

III. Setting by Alarm Type

Command: (**no**) **alarm output alarmtype** *type_value*

This command can enable the user to set alarm output by alarm type.

type_value: alarm type. There are five types: Communication alarm, service_quality alarm, process_error alarm, equipment alarm and environmental alarm. It is only necessary to input the English word indicating the corresponding type directly.

IV. Setting the Output of All Alarms

Command: (**no**) **alarm output all**

After you have made a series of output settings, you may not remember the output status. Therefore, the following command can be used for setting the output flags for all alarms.

V. Querying Command Execution Result

You can use command **show alarm content** *alarmid* to show whether the alarm is outputted to command line, and to verify the command execution.

alarmed: Alarm ID, ranging 52–1572886.

Caution:

- The settings are effective for all command line terminals, that is, whether an alarm will be reported to all the terminals or not be reported to any terminal.
- The alarm output mask function mentioned here is ineffective for NMS, and NM terminal will provide other abundant alarm filtration functions.
- The setting of alarm output command has no impact on alarm generation. The alarms generated by the system will still be recorded, and the user can query the records by using alarm history record query command.
- Several alarm output setting methods provided will affect each other, while whether a certain type of alarms will be outputted depends on the last setting.
- The output flag of recovery alarms is the same as that of fault alarms. The system performs this function automatically. That is, if the user sets an output flag for the fault alarm, the system will set the corresponding recovery alarm with the same output flag. In a similar way, when setting the recovery alarm output flag, the corresponding fault alarm output flag will keep consistent.

7.6 Setting RTCP Alarm Threshold

The real-time transport control protocol (RTCP) packet contains the statistical results of the round-trip delay, delay jitter and packet loss ratio of the real-time transport protocol (RTP) channel. A RTP packet is voice packet generated in a call.

When the operational values of the system exceed the RTCP packet threshold, the thresholds of the round-trip delay, delay jitter and packet loss ratio of the RTP channel, or the threshold of the interval between sending two RTCP packets, an alarm is generated. The related commands are listed in Table 7-16.

Table 7-16 Commands related to RTCP alarm thresholds

Operation	Command
Set RTCP threshold	IAD2000(config)#**rtcp_para** { **alarmthreshold** *alarmthreshold* | **lost** *lost* | **delay** *delay* | **jitter** *jitter* | **timer** *timer* }
Show RTCP threshold status	IAD2000>#**show rtcp_para**

The parameters of the commands are listed in Table 7-17.

Table 7-17 Parameters of commands

Item	Description
alarmthreshold	Threshold of alarm RTCP packet, that is, an alarm is generated after the parameters *delay*, *jitter* and *lost* of how many RTCP packets in a row exceed the thresholds. The value range is 0 to 5, and the default value is one packet. If it is set to 0, it means no alarm is generated regardless of the network status; that is, the alarm and log function of RTCP is disabled.
delay	RRound-trip delay of the RTP channel. The value range is 50 to 1,000 milliseconds.
jitter	Delay jitter of the RTP channel. The value range is 10 to 200 milliseconds.
lost	Packet loss ratio of the RTP channel. The value range is 0%–20%.
timer	The time interval between sending RTCP packets. The value range is 0 to 60 seconds.

Example:

Set the RTCP alarm thresholds as follows:

```
IAD2000(config)#rtcp_para alarmthreshold 2 lost 10 delay
100 jitter 100 timer 10

IAD2000(config)#
```

Query the current RTCP threshold settings:

```
IAD2000(config)#show rtcp_para
lost rate of RTP channel          :10%
delay of RTP channel              :100ms
```

```
jitter of RTP channel              :100ms
timer length of RTCP channel       :10s
alarm threshold of RTCP channel    :2
IAD2000(config)#
```

7.7 Patch Management

7.7.1 Overview of Patch

IAD108 is required to run without interruption for a long time. To amend some software problems or add new functions, you need to modify the host software without interrupting the service, that means patch the host software.

In IAD108 the patches have three statuses.

- Deactive: The patch has been added into the host but not activated, and the patch code takes no effect.
- Active: The patch code takes effect and its status can be modified by executing commands patch start and no patch active.
- Running: The patch is in running status and can only be deleted rather than be deactivated.

Note:

- The difference between Running status and Active status is that the patches in Running status can automatically recover to Running status after the system is rebooted, while those in Active status will become Deactive after rebooting.
- The Active status can be regarded as the “trial running” of the patch. Through the trial running you can check whether the expected functions are achieved. Only the patches passed the trial running test can be used normally.

The commands provided by the system for patching are listed in Table 7-18.

Table 7-18 Commands used for patching

Command	Description
patch active	It is used to activate the patch.
patch deactive	It is used to deactivate the patch.
patch start	It is used to run the patch.
patch remove	It is used to delete the patch.
show patch	It is used to display the information of the patch.

7.7.2 Steps of Operating Patches

Patches can be operated in the following sequence:

1) Load the patch file to CVP board. If the loading succeeds, you can check the information of the patches by executing command **show patch**.
2) After checking that the patch is correct, you can execute command **patch active** to activate the patch. If the activation succeeds, you can verify the functions of the patch or test the functions.
3) After verifying the functions, you need to run the patch normally. To do this, you need to execute command **patch start** to transfer the patch status to the Running status.

7.8 Network Test Tools

7.8.1 ping

In user mode, **ping** command can be used to check the connection state of the system and whether the host is reachable. The format of the command is **ping** *hostip*, between which there can be one or multiple parameters, as shown in Table 7-19.

Table 7-19 Parameters of **ping** command

Parameter	Meaning of parameter
-c	Sets the number of ICMP (Internet Control Message) ECHO_REQUEST messages sent.
-d	Sets “socket” debugging function.
-i	Sets that ECHO_REQUEST message is sent to the directly -connected network through ping without routing.
-p	Sets the fill byte of ECHO_REQUEST message, for example, -p 0xff fills the message to 000000ff

Parameter	Meaning of parameter
-q	Except statistics, other detailed information is not displayed.
-s	Sets the length of ECHO_REQUEST message.
-t	Sets the time-out time of waiting for the response of ECHO_REQUEST message.
-v	Displays the received non ECHO_RESPONSE ICMP messages. It is not displayed by default.

Example:

```
IAD2000(config)#ping -c 10 10.72.54.100
  PING 10.72.54.100: 56 data bytes, press CTRL_C to break
  Reply from 10.72.54.100: bytes=56 Sequence=0 ttl=119
time = 0 ms
  Reply from 10.72.54.100: bytes=56 Sequence=1 ttl=119
time = 0 ms
  Reply from 10.72.54.100: bytes=56 Sequence=2 ttl=119
time = 0 ms
  Reply from 10.72.54.100: bytes=56 Sequence=3 ttl=119
time = 0 ms
  Reply from 10.72.54.100: bytes=56 Sequence=4 ttl=119
time = 0 ms
  Reply from 10.72.54.100: bytes=56 Sequence=5 ttl=119
time = 0 ms
  Reply from 10.72.54.100: bytes=56 Sequence=6 ttl=119
time = 0 ms
  Reply from 10.72.54.100: bytes=56 Sequence=7 ttl=119
time = 0 ms
```

```
  Reply from 10.72.54.100: bytes=56 Sequence=8 ttl=119
time = 0 ms
  Reply from 10.72.54.100: bytes=56 Sequence=9 ttl=119
time = 0 ms

  --- 10.72.54.100 Ping statistics ---
  10 packets transmitted
  10 packets received
  0.00% packet loss
  round-trip min/avg/max = 0/0/0 ms

IAD2000(config)#
```

7.8.2 tracert

In user mode, command **tracert** is used to test the gateways through which data packet is sent from the host to destination. It is mainly used to check whether the network connection is reachable, and analyze where a fault occurs in the network.

The format of the command is **tracert** *hostip*, between which there can be one or multiple parameters, which are shown in Table 7-20.

Table 7-20 Parameter table of **tracert** command

Parameter	Meaning of parameter
-d	Sets the debugging printing switch.
-f	Sets the minimum value of TTL
-m	Sets the maximum value of TTL

Parameter	Meaning of parameter
-q	Sets the number of detection packets
-w	Sets time-out time

The procedure of executing **tracert** is: first send a data packet with TTL as 1. Therefore, an ICMP error message is returned for the first hop to indicate that the data packet cannot be sent (since TTL is time out), after that, the data packet is resent, with TTL as 2. Similarly, TTL timeout is returned for the second hop. The procedure is carried on constantly until reaching the destination. The purpose of carrying out these procedures is to record the source address of each ICMP TTL timeout message, so as to provide the path through which an IP data packet reaches the destination.

7.8.3 Example for Command Ping

I. Networking

As shown in the following diagram, IAD108 maintenance port is connected to the maintenance terminals 1 and 2 through Local Area Network (LAN). The IP addresses of the three parties respectively are: 172.21.100.16, 172.21.50.51, and 172.21.50.84.

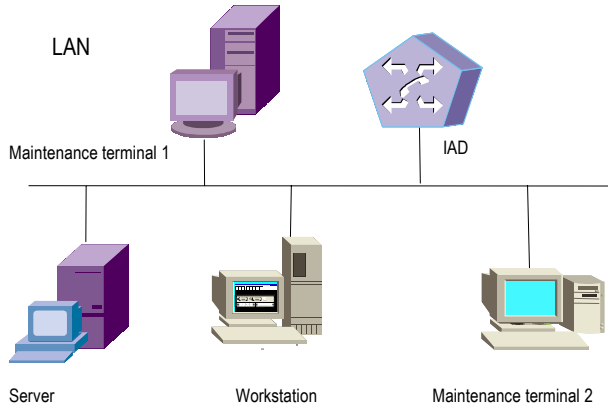


Figure 7-1 Networking for case 1

II. Fault Phenomenon

Sometimes the maintenance terminal 1 can be connected to IAD108 through Telnet, and sometimes it cannot. The maintenance terminal 2 can be normally connected to IAD108 through Telnet.

III. Processing Procedure

Connect the maintenance terminal 2 to IAD108 through Telnet. Execute **Ping** command to check whether the link between IAD108 and the maintenance terminal 1 is normal.

1) Adopt the default parameter value of **ping** command to ping the maintenance terminal 1.

```
IAD2000(config)#ping 172.21.50.51
```

```
  PING 172.21.50.51: 56  data bytes, press CTRL_C to break
  Request time out
  Request time out
  Request time out
  Request time out
  Request time out

  --- 172.21.50.51 Ping statistics ---
  5 packets transmitted
  0 packets received
  100.00% packet loss

IAD2000(config)#
```

2) Send 10 ping messages continuously to check whether there exists packet loss, that is, to adopt the parameter c=10 to ping the maintenance terminal 1. Finally, only 5 messages can reach the destination. There exists serious packet loss. It might be caused by poor network quality, busy network, or interference.

```
IAD2000(config)#ping -c 10 172.21.50.51
  PING 172.21.50.51: 56  data bytes, press CTRL_C to break
  Request time out
  Reply from 172.21.50.51: bytes=56 Sequence=0 ttl=128
time = 0 ms
  Request time out
  Reply from 172.21.50.51: bytes=56 Sequence=3 ttl=128
time = 0 ms
  Request time out
  Reply from 172.21.50.51: bytes=56 Sequence=5 ttl=128
```

```
time = 0 ms
  Request time out
  Request time out
  Reply from 172.21.50.51: bytes=56 Sequence=7 ttl=128
time = 0 ms
  Reply from 172.21.50.51: bytes=56 Sequence=8 ttl=128
time = 0 ms

  --- 172.21.50.51 Ping statistics ---
  10 packets transmitted
  5 packets received
  50.00% packet loss
  round-trip min/avg/max = 0/0/0 ms

IAD2000(config)#
```

7.8.4 Example for Command tracert

I. Networking

Figure 7-2 shows the networking:

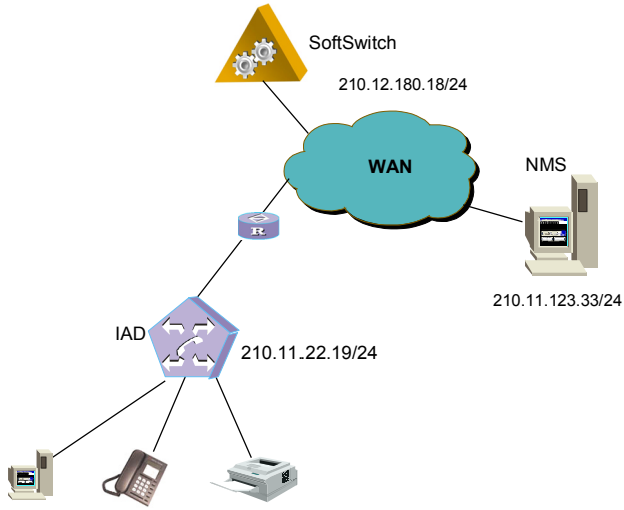


Figure 7-2 Networking diagram

II. Processing Procedure

Telnet the IAD108, and run the command **tracert** in user mode to check the network connection between the IAD108 and the SoftSwitch:

```
IAD2000(config)#tracert 210.12.180.18
 traceroute to 210.12.180.18 max hops 30 ,packet 40 bytes
  press CTRL_C to break
 1      1 ms     <10 ms   <10 ms    210.11.22.254
 2      1 ms     2 ms     2 ms      210.110.0.17
 3      1 ms     1 ms     1 ms      210.11.180.18
Trace complete.
```

```
IAD2000(config)#
```

From the above result, you can see which gateway devices the signal has passed through on its way from the source device (IAD108) to the destination (MGC). This is very helpful in analyzing the network conditions.

Chapter 8 Troubleshooting

This chapter first introduces common means of locating IAD faults so that you can master simple fault-locating methods. It then gives some examples on IAD faults for your reference.

8.1 Common Fault-locating Means

8.1.1 Showing Important System Information

I. Showing Version

Obtaining the software version of the equipment is the basis of locating its faults. If the software the IAD108 uses is not the latest version, some of its problems may have been solved in a subsequent version. In this case, you can locate some problems from the version number and get corresponding solutions.

By carrying out the **show version** command in the user EXEC mode, you can show the software and hardware version of the equipment.

```
IAD2000#show version
  Equipment type            : IAD108
  Main Board PCB version    : AG21CSPA VER.A
  Software version          : IAD2000V200R002B01D031
  BIOS version              : 506
  SLIC version              : (U35-U38)015
  CPLD version              : (U16)100
  DSP version               : (U34)V100R1C1B23D10
IAD2000#
```

II. Showing Interface Status

Once there is a system fault leading to service failure, you should first check MG interface information. Calls can be made only when the interface status is normal. Otherwise, the subscriber hears the busy tone after hooking off.

In privilege mode, you can use the **show mg attribute** command to show the MG status.

```
IAD2000#show mg attribute

-------------------------------------------------------
---------
  MGID       Protocol         Codetype         DomainName
  0          MGCP              text             iad53.com
  Transmode   IADPort           IADIP            Interface
state
  UDP        2427             172.21.100.53     Interface
normal
  MGCport    MGCIP/DomainName               InterfaceName
  2727        172.21.1.1                          aaln

-------------------------------------------------------
-----------
```

III. Showing Port Status

By showing the port status, you can check the status of each subscriber. The status of a port in normal use is idle or busy.

You can use the **show port state** command in the user EXEC mode to show the port status:

```
IAD2000#show port state
{ <cr>|portid<U><0,7> }:

Command:
        show port state

-------------------------------------------------------
   Port  PortType State    ServiceType   ServiceState

-------------------------------------------------------
     0    PSTN    Idle    Instant service   Start service
     1    PSTN    Busy     IP SPC           Start service
     2    PSTN    Idle    Instant service   Start service
     3    PSTN    Idle    Instant service   Start service
     4    PSTN    Idle    Instant service   Start service
     5    PSTN    Idle    Instant service   Start service
     6    PSTN    Idle    Instant service   Start service
     7    PSTN    Idle    Instant service   Start service

-------------------------------------------------------
IAD2000#
```

IV. Showing Time of System Restarting

In privilege mode, you can use the **show clock** command to show when the system is reset and restarted.

```
 IAD2000#show clock
-------------------------------------------------
  System startup date: 2004-08-17 time: 14:48:49
  Current date: 2004-08-18
```

```
  Current time: 09:27:53
-------------------------------------------------
IAD2000#
```

V. Showing IP Address and Route Information

When a network fault occurs, you need to show the following information. Use the four commands specified in Table 8-1 to locate the fault.

Table 8-1 Common commands to show information on network faults

Function	Command
Showing IP address	IAD2000>show ip address
Showing route information Incorrect route information may lead to interface faults, monologs, or communication failures.	IAD2000#show ip route
Showing ARP entry in IAD	IAD2000>show arp entry

VI. Showing RTP Statistical Information

You can carry out the **show rtp stat** command to show information on media stream.

```
IAD2000(config)#show rtp stat 2/6
```

The parameters displayed by this command have the following meanings as listed in

Table 8-2 Parameters in the result

Item	Description
Number of packets received (sent)	It equals call duration (second) x 1000/length of packet received (sent).
Codec algorithm	0: G.711u
	4: G.723 high
	8: G.711A
	18: G.729
	20: G.723 low
Jitter	In a good network condition, the jitter is usually lower than 30ms.
Number of lost packets	Query many times, and the difference between numbers of sent packets and received packets is stable.

8.1.2 Showing Alarms

Alarm information is part of the history records on equipment operation. By analyzing alarm information, you can predict problems that may arise in the running of the equipment. Note that when the IAD108 encounters a power failure and is restarted, the alarm records saved before will be lost.

The command to show all alarms is **show alarm record all**. For other commands to show alarms, refer to the help information.

During the running process of IAD108, pay attention to the following alarms.

I. System Start Alarm

This alarm tells you the system start time and whether the system was reset while it was running. The following is an example.

```
ALARM 4 INFO MAJOR 0x00000336 ----- 2004-08-18 09:37:34
  ALARM NAME : device start
  PARAS INFO : device start
 DESCRIPTION : device start
      REASON : none
      ADVICE : none
--- END
```

II. Interface Interruption/Recovery Alarm

Interface interruption is generally caused by network conditions. When interface interruption occurs, no phone calls can be made. If you hear busy tone or no tone after off-hook, you should first check if there is an interface interruption alarm.

If multiple IAD108 devices in the same area generate interface interruption alarms almost at the same time, the problem is usually caused by the bearer network. It is that normal each system startup is accompanied by an interface recovery alarm.

The following is an example.

```
  ALARM 5 RESTORE MAJOR 0x00170105 COMMUNICATION
2004-08-18 09:38:03
    ALARM NAME : MG interruption restoration
    PARAS INFO : MG ID: 0
   DESCRIPTION : MG restore
        REASON : MG is normal
        ADVICE : None
```

```
--- END
```

8.1.3 Capturing Network Packets

To locate faults in a Voice over IP (VoIP) device by capturing packets, we recommend Sniffer pro 3.0.

All IAD108 signaling and voice data are borne on the user datagram protocol (UDP). The protocol stack architecture is as shown in Table 8-3. The key protocols are RTP and MGCP.

Table 8-3 The UDP stack

Telnet remote maintenance	Voice		Call control
Telnet	RTP	RTCP	MGCP
TCP	UDP		
IP			
MAC			

8.1.4 Tracing Signaling

In diagnose mode, use the following command to enable the signaling tracing switch, and then locate the fault through signaling tracing.

trace { **phyport** *phyport* | **status** *tracestatus* | *protocoltype tracerange* **phone** *phonenumber* | **port** *portno* | **terminal** *terminalid* **command** *commandname1 commandname2 commandname3 commandname4 commandname5* }

The meanings of the parameters are listed in Table 8-4.

Table 8-4 Parameters of command

Item	Description
phyport	Physical port number, ranging 0–7.
tracestatus	Signaling tracing status, with value as “offline” or “online”.
protocoltype	Signaling tracing protocol, with value as “h248” or “mgcp”.
tracerange	Range of signaling tracing commands, with values as “allcmd” or “partcmd”.
phonenumber	Telephone number, ranging 1–16 digits.
portno	Physical port number, ranging 0–7.
terminalid	MG terminal ID, ranging 0–8.
commandname	Command used for tracing the protocol.

8.2 IAD Port ID Error Leads to Call Failure.

8.2.1 Symptom Description

In the IP access network (IPAN) networking, a subscriber under a port of the IAD hooks off and hears the dialing tone, but cannot dial successfully. Meanwhile, other ports are normal.

8.2.2 Causal Analysis

If some ports are unavailable while others are normal, it means the IAD has been successfully registered and the fault is caused by a subscriber port ID error. The error may be in the User ID on the ETG, the corresponding relations between the L3 addresses on the ETG and that on the switch, or the Interface ID (aaln/X) on the IAD.

Perform the following steps to troubleshoot the port error:

1) Carry out the show mg ag all command on the ETG to check if the corresponding IAD has been successfully registered.
2) Carry out the show port command on the IAD to check if the port and the corresponding subscriber phone set are normal. If they are not normal, it is usually caused by subscriber board faults.
3) If the IAD port is normal, carry out the show pstn-port command on the ETG to show the IAD port status. If the status is not normal, it is generally because the L3 address does not correspond or the subscriber data has not been configured.

Note:

- Different IADs may have different models and are produced by different manufacturers; therefore, their numbering modes may be different. The port IDs of the IAD108 starts with 0.
- The IP console must correspond to two user IDs, and the first port ID must be an even number.

8.2.3 Processing Procedure

According the fault phenomena and causes analyzed above, the processing procedures are as follows.

1) Make test calls to confirm that some port cannot process dialing but other ports can. Then check the external line to rule out related causes.

2) Carry out the show port command on the IAD to show the IAD port. If the port is normal, carry out the show pstn-port command on the ETG to show the IAD port status is normal.
3) Closely examine the interface ID on the IAD, and you can find that the ID of the first port is aaln/1; however, the ID of the first port of the IAD108 should be aaln/0. Other ports are numbered in order. After the modification is saved, test calls show that the problem remains.

Carry out the show user-endpoint-info-cfg command on the ETG, and you will find that the user ID corresponding to the IP console is 32, and the user ID corresponding to the first subscriber port is 33. Re-collate the user IDs. Make the IP console correspond to the user ID of 32. Leave 33 unused. Make the first subscriber port correspond to 34. Number other ports by order. Save the data. Make test calls, and you will find the problem is solved.

8.2.4 Suggestion and Summary

In deployment, you should understand the parameters on the switch, ETG and IAD, as listed in Table 8-5.

Table 8-5 Parameters on the switch, ETG and IAD

Item	Description
L3 address	Both the switch and ETG have this parameter. The L3 addresses on the two devices correspond to each other on a one-to-one basis. The switch uses the L3 address to correspond to the end subscriber on the IAD port through the ETG.

Item	Description
User ID	It is also called subscriber number. Only the ETG has this parameter. Corresponding relations between the L3 address on the switch and the IAD port ID are achieved through UserID. The process is as follows: Corresponding relations between UserID and L3 address are achieved through “add user-v5-info-cfg”; corresponding relations between UserID and IAD port ID “aaln/X” through table “add user-endpoint-info-cfg”.
Interface ID	Its format is aaln/X (X is an integer from 0 to 32). This parameter exists in the ETG and IAD. It corresponds to the subscriber port ID on the IAD. The port IDs of the IAD108 starts with aaln/0.

8.3 Echo Occurs in PSTN Calls.

8.3.1 Fault

In a network comprised of devices from different manufacturers, the IAD is allocated with a private IP address. It connects with the metropolitan area network (MAN) through network address translation (NAT) and networks with the BISC software of company S.

The IAD is the IAD108. Make a PSTN call from a phone set under the IAD. The communication on the IAD side is normal, but there is an echo on the PSTN side.

8.3.2 Cause

Analysis of on-site packet capture result shows that, in the signaling delivered by the softswitch, both “e:on” and “s:on” are on. The packet is as follows:

2b: [131][14:09:15.190]Recieve From MGC:CRCX 12762 aaln/01@172.17.18.36 MGCP 1.0C: 1M: inactiveL: p:10, a:PCMA,

b:64, e:on, s:onQ: loop,processR: G/ft(N),G/mt(N)S: X: 1200177206000C00

The softwitch of company S enabled echo cancellation (EC), and EC operates on the peer end; therefore, an echo is heard on the PSTN side.

8.3.3 Processing Procedure

According to the internal flow of the IAD and SoftX3000 of Huawei, when the IAD networks through NAT, EC and VAD on the IAD side should be set to “off”, and they should not be seen in the signaling returned by the IAD.

After EC and VAD on the softswitch of company S are disabled, the fault disappears and communication returns to normal.

8.4 Call Fails After Telephone Ringing

8.4.1 Fault

A carrier's networking consists of the SoftX3000 plus IAD and TMG8010. When an IAD user calls a user of other carriers, the call needs to go out through the TMG8010. In the local equipment room there are an IAD and TMG8010, which connect to the LAN Switch and router. The IAD can successfully calls a subscriber of other non-local carriers. If the subscriber calls a subscriber of other local carriers, the phone set of the callee can ring. However, when the callee hooks off, there is no tone, and neither side can communicate.

8.4.2 Cause

The call signaling flow of the IAD subscriber is “IAD--SoftX3000--TMG8010—other carriers”. Analysis of the fault

shows that the phone set of the callee can ring, which means that communication between IAD and SoftX3000 and that between TMG8010 and SoftX3000 are normal.

The call flow of the IAD subscriber is “IAD--TMG8010—other carriers”. Since calls from the IAD to a non-local TMG8010 is normal, communication between IAD and non-local TMG8010 is normal. Since calls from the IAD to other local carriers are abnormal, the problem should be that communication between IAD and local TMG8010 is abnormal.

Check the IP address settings of the IAD and TMG, you can see that the IP address of the IAD is set to 10.14.96.103/26, while that of the TMG8010 is set to 10.14.96.101/29. The setting of the mask of the TMG8010 is too low, which leads to communication failures between TMG8010 and IAD.

8.4.3 Processing Procedure

According the fault phenomena and causes analyzed above, the processing procedures are as follows.

1) The address of the SoftX3000 can be pinged through from both the IAD and the TMG8010.
2) Make the IAD and the TMG8010 ping each other. If they cannot be pinged through, it means the circuit is not through.
3) Modify the mask of the TMG8010 to 26 digits. Then the fault disappears.

8.5 Monolog

8.5.1 Fault

Monolog occurs when the IAD and OPENEYE directly call each other. The voice from the IAD side cannot be heard on the OPENEYE (SIP-based). After various models of IAD, including 101, 102 and 108, are tried, the problem remains. However, communication between IADs is normal, both IAD and OPENEYE are successfully registered, and their interaction with the softswtich is normal.

8.5.2 Cause

Since the IAD communicate with other IADs normally, IAD hardware faults can be ruled out. You can consider replacing the PC of the OPENEYE.

8.5.3 Processing Procedure

According the fault phenomena and causes analyzed above, the processing procedures are as follows.

1) After installing the OPENEYE in another PC, communication returns to normal.
2) Check the faulty PC. It is installed with two network cards. One network card (hereinafter referred to as card 1) is integrated on the mainboard; the microphone and headphone interface are also integrated on the mainboard. Another network card (hereinafter referred to as card 2) is plugged in the extended slot of the mainboard.

The IP addresses are planned as listed in Table 8-6.

Table 8-6 Planning of IP address

Item	Description
Card 1	The IP address is 10.22.11.9/24, and the gateway is 10.22.11.254. This network port is used to catch the packets of the MGC (whose address is 10.22.11.2).
Card 2	The IP address is 10.22.3.201/24, and the gateway is 10.22.3.254.
Peer IAD	The IP address is 10.2.128.65/28. This address can be pinged through from card 1 and card 2.

When card 2 is selected for the OPENEYE, monolog occurs when the OPENEYE and IAD call each other. Voice can be heard on a phone set under the IAD, but the peer-end voice cannot be heard on the OPENEYE.

When card 1 is selected for the OPENEYE, communication is normal.

When the OENEYE is installed in a PC with two network cards, the incoming voice stream must be processed.

8.6 Voice Quality Deterioration

8.6.1 Fault

Jitters occur in communication and voice cannot be heard clearly.

8.6.2 Cause

Since only a few IADs in this office operate like this, it can be seen that this is a network fault.

8.6.3 Processing Procedure

According the fault phenomena and causes analyzed above, the processing procedures are as follows.

1) The network blocks ping function. A ping test cannot be conducted.
2) Test the equipment when it is idle. If the problem remains, network bandwidth problems can be ruled out.
3) Check the negotiation status of the uplink interface and find that it is set by negotiation to 10M semi-duplex. Maybe it is set to full-duplex on the peer end and to adaptive on our side, and by negotiation it is set to semi-duplex. Modify it to full-duplex. However, the problem remains.
4) Confirmation shows that mode of the photoelectric transducer is 10M semi-duplex. After it is modified to full-duplex, communication becomes normal.

8.6.4 Suggestion and Summary

Voice communication often generates a bidirectional network traffic. The semi-duplex mode only allows a traffic in one direction at one time, which leads to the problem in voice quality. Where possible, the full-duplex mode should be set.

8.7 IAD Echo

8.7.1 Fault

When the IAD subscriber is in a conversation, there is an echo, and the voice is intermittent.

8.7.2 Cause

This problem is generally caused by the following factors: on the IAD or TG, the echo cancellation parameter is disabled, the silence detection parameter is enabled, or the receiving/sending gain parameter is unreasonably set.

The echo source is generally caused by the peer end. If the IAD subscriber hears the echo, you should adjust the echo cancellation and receiving/sending gain parameters on the TG/ETG. If the PSTN subscriber hears the echo, you should adjust the echo cancellation and receiving/sending gain parameters on the IAD side.

8.7.3 Processing Procedure

I. Adjusting Echo Cancellation Switch

If the PSTN subscriber hears the echo, carry out the **show mg system-parameter** command on the IAD to show the IAD system parameters, and carry out the **mg system-parameter** command to modify them.

Parameter 8 “Dsp echo check” should be set to 1 (enabled).

Parameter 9 silence detection “Dsp silence reduce” should be set to 0 (disabled).

If the IAD subscriber hears the echo, it may be caused by the TG/ETG. In this case, you need to modify the echo cancellation parameter on the TG/ETG as follows:

Carry out the **modify ipp-ch** command to modify echo cancellation on every board. Enable parameter 4. If the echo remains, adjust parameter 16 and increase its value. This parameter indicates

the buffer value of echo cancellation. Its value range is 0 to 15, and 8 ms is a level.

II. Adjusting Receving/Sending Gain

Normally, the echo problem can be solved after the above parameter adjustments. If the echo or cut voice (intermittent communication) remains, you need to adjust the gain on the two sides. This problem is caused by improper gain settings which affect EC.

The basic principle for gain adjustment is that the different between the sending gain of the TG and that of the IAD should be as little as possible. In this way, the EC intermittence can be reduced.

Generally, we recommend the following settings:

- Sending gain and receiving gain of the TG be both set to 0db.
- Sending gain and receiving gain of the IAD be set to –3.5 and 0 respectively.

Carry out the **mg system-parameter** command to adjust the IAD gain. The gain is parameters 3 and 4 (parameter 3 is the DSP input gain, while parameter 4 is the DSP output gain).

Carry out the **modify ipp-ch** command to adjust the TG gain. Parameters 14 and 15 should be modified. The method to modify the gain is as follows:

1) The size of the gain is adjustable from -14 dB to +6 dB. The variation step is 0.1 dB. If the step is set to 1, the adjustable gain range is from -140 to +60. To avoid negatives, set its value range as from 0 to 200.
2) The relationship between the gain parameter set by the subscriber and the actual gain is: actual gain = (gain

parameter-140)/10. For example, if the subscriber sets the parameter to 120, the actual gain is (120-140)10 = -2 dB. The default value of this parameter is 140, which means the default gain is 0 dB.

Generally, the above procedure can solve the echo and cutting voice problem.

8.8 Voice Abnormality

8.8.1 Fault

Voice is too high or too low for IAD subscribers.

8.8.2 Cause

Too high or too low voice is related to system gain. This problem can be solved by adjusting the sending gain of the peer end and the receiving end of the local end, including the DSP input/output gain of the voice pinch board, TG gain, and the receiving/sending gain of the subscriber physical port. The functions of the gains are as follows:

- The voice quality can be remarkably improved by adjusting the receiving/sending gain of the IAD subscriber physical port.
- The voice quality can also be improved by adjusting the DSP input/output gain, but the effect is not remarkable.
- Adjusting the TG gain has an impact on the global office; therefore, it is not recommended.

8.8.3 Processing Procedure

The receiving/sending gain of the IAD subscriber physical port can be adjusted according to international standards and actual network quality. The usual recommendations are as follows.

Chinese national standard recommends that the sending/receiving gain of the local network should be 0/-3.5 (high gain), and that of the toll network is 0/-7.

International standard recommends the narrowband sending/receiving gain should be 0/-7.

Because the voice of the IAD is received and sent in RTP packets, it is recommended that the receiving/sending gain of the IAD subscriber physical port be set to0/-7 (low gain).

Appendix A Command List

Command name	Function	Mode
A		
alarm level	Setting alarm level.	Global Config
alarm output	Setting command line output flag of alarm.	Global Config
alarm statistics	Setting alarm statistics flag.	Global Config
alarm statistics clear	Clearing alarm statistics table.	Privilege
alarm threshold	Setting alarm statistics threshold.	Global Config
B		
backup data	Backing up database file.	Privilege
backup running-config	Backing up operation and configuration.	Privilege
backup startup-config	Starting the backup of configuration file.	Privilege
banner incoming	Configuring this office information and contact telephone number.	Global Config
baudrate	Setting baud rate of the serial port.	Privilege
C		
clear	Clearing the statistics information of the LAN Switch port.	LAN Switch
clock set	Setting system time.	Privilege

Command name	Function	Mode
cls	Clearing the screen.	User
configure terminal	Entering global config mode.	Privilege
D		
data set autosave	Setting the automatic saving switch for configuration data.	Global Config
data set autosave interval	Setting the automatic saving interval for configuration data.	Global Config
dhcp disable	Disabling DHCP function.	Global Config
dhcp enable	Starting DHCP function.	Global Config
dhcp renew	Refreshing the configuration of IP address.	Global Config
disable	Exiting from current command mode and entering user mode.	Privilege
dns domain-name	Configuring DNS domain name	Global Config
dns server	Configuring the IP address of DNS server.	Global Config
dsp reset	Resetting the DSP chip.	Global Config
dsp-channel prohibit	Prohibiting/unprohibiting DS channel.	Global Config
duplex	Setting the LAN Switch interface to work in duplex mode.	LAN Switch
E		
ec set	Configuring echo cancellation function.	Advance
echo	Enabling the echo of command.	User

Command name	Function	Mode
enable	Entering privilege mode.	User
endservice	Terminating the service.	Global Config
exit	Exiting from the current command mode to the previous command mode or exiting from the configuration environment.	Any mode
F		
fax cleanreport	Clearing the statistics of fax event	Global Config
fax gain-factor	Setting the fax sending level parameter	Global Config
fax gain-level	Setting the fax sending level	Global Config
fax net-jitter-threhold	Setting the network jitter threshold	Global Config
fax port-add-2	Whether ass 2 to the fax port	Global Config
fax rate	Setting fax rate	Global Config
fax relay	Setting fax mode	Global Config
fax support-mode	Setting fax support mode	Global Config
fax t38-redundancy	Configuring T38 fax redundancy packet	Global Config
fax train-mode	Configuring fax train mode	Global Config
flow-control	Setting flow control over the LAN Switch interface.	LAN Switch
ftpserver	Configuring FTP server.	Global Config
H		

Command name	Function	Mode
help	Calling the global help information of command line.	User
help-mode	Enabling the input memorizing function.	User
history size	Setting the lines of history commands stored in the buffer.	User
hostname	Modifying the command line prompt.	Global Config
I		
iadms	Configuring the information list of IADNMS.	Global Config
infolevel cli	Setting output level of command line information.	Global Config
infolevel nms	Setting output level of NMS information.	Global Config
infolevel syslog	Setting output level of log host information.	Global Config
infoswitch cli	Setting the output switch of command line.	Global Config
infoswitch nms	Setting the output switch of NMS information.	Global Config
infoswitch syslog	Setting the output switch of log host information.	Global Config
ip address	Setting the system's IP address.	Global Config
L		
language	Switching the language mode.	User

Command name	Function	Mode
LAN Switch	Entering the LAN Switch configuration mode.	Privilege
load data	Loading board data file.	Privilege
load program	Loading board program.	Privilege
load system	Loading the system.	Privilege
loghost active	Activating the configuration of log host.	Global Config
loghost add	Adding a log host.	Global Config
loghost delete	Deleting a log host.	Global Config
M		
mg attribute	Configuring MG attribute.	Global Config
mg backup	Backing up MGC	Global Config
mg register-key	Configuring MG interface registration key.	Global Config
mg register-MgID	Authenticate AuthMGID	Global Config
mg register-MgKI	Authenticate AuthKI	Global Config
mg register-mode	Authentication mode	Global Config
mg reset	Resetting MG and registering again.	Global Config
mg shutdown	Turning off MG	Global Config
mg software-parameter	Configuring MG software parameters.	Global Config
mg system-parameter	Configuring MG system parameters.	Global Config

Command name	Function	Mode
mgcp	Setting MGCP parameters.	Global Config
mgcpstatresult clear	Clearing signaling statistics result.	Global Config
mguser add	Adding an IAD user.	Global Config
mguser batadd	Batch-adding IAD users.	Global Config
mguser batdel	Batch-deleting IAD users.	Global Config
mguser del	Deleting IAD users.	Global Config
mguser modify	Modifying IAD users.	Global Config
monitor	Setting LAN Switch monitoring interface.	LAN Switch
multicast enable	Enabling a multicast group.	LAN Switch
multicast group	Configuring the MAC address or LAN Switch interface of a multicast group.	LAN Switch
N		
negotiation-auto	Setting auto-negotiation mode of LAN Switch interface.	LAN Switch
no alarm output	Clearing command line output flag of alarms.	Global Config
no alarm statistics	Clearing alarm statistics flag.	Global Config
no baudrate	Restoring the baud rate of serial port to default value.	Privilege
no dsp -channel prohibit	Unprohibiting DSP channel.	Global Config
no ec set	Restoring the default configuration of echo cancellation attribute.	Advance

Command name	Function	Mode
no echo	Disabling the echo function.	User
no flow-control	Canceling the traffic control over the Ethernet interface.	LAN Switch
no help-mode	Disabling the input memorizing function.	User
no iadms	Deleting the IADMS.	Global Config
no loghost active	Deactivating a log host.	Global Config
no loopback	Stopping the loopback of the port.	LAN Switch
no mgcptrace	Stopping the signaling tracing of the endpoint.	Global Config
no monitor	Canceling the LAN Switch's monitoring network interface.	LAN Switch
no multicast enable	Deactivating the multicast group.	LAN Switch
no multicast group	Deleting the MAC address or Ethernet interface of a multicast group.	LAN Switch
no patch active	Deactivating a patch.	Privilege
no priority	Restoring a network interface to normal priority.	LAN Switch
no scroll	Setting the screen display as manual scroll.	User
no shutdown	Turning on the Ethernet interface.	LAN Switch
no slic set	Canceling the configuration of user attribute.	Advance
no smart	Disabling the interaction function.	User
no spc release	Establishing an SPC connection.	Global Config

Command name	Function	Mode
no terminal hold	Unlocking the terminal.	User
no terminal timeout	Disabling the function that when the terminal timeouts it exits from the system.	User
no timeout	Closing the terminal timeout control switch.	User
no trunk enable	Deactivating a TRUNK group.	LAN Switch
no trunk group	Deleting the LAN Switch interface of a TRUNK group.	LAN Switch
no uplink	Configuring a network interface as non-uplink interface.	LAN Switch
no user apdinfo	Deleting the user's appendix information.	Global Config
no user name	Deleting a user.	Global Config
no vlan	Deleting all the ports in a VLAN.	LAN Switch
P		
patch active	Activating a patch.	Privilege
patch remove	Deleting a patch.	Privilege
patch start	Running the patch normally, after rebooting it can run normally.	Privilege
ping	Checking the network connection or whether the host is reachable.	User
priority	Configuring a network interface as with high priority.	LAN Switch
pstnport attribute set	Setting the PSTN interface attribute	Global Config

Command name	Function	Mode
pstnport attribute batset	Batch-adding the PSTN interface attribute	Global Config
R		
reboot	Rebooting the system.	Privilege
reset	Resetting the gateway/board/port/MG interface.	Global Config
reset	Resetting the LAN Switch.	LAN Switch
reset interface	Resetting the LAN Switch interface.	LAN Switch
restore default-config	Restoring the system default configuration data.	Global Config
S		
scroll	Enabling the auto scrolling of the screen.	User
show alarm content	Querying the alarm configuration information.	User
show alarm list	Showing alarm basic information.	User
show alarm record	Querying history alarm records.	User
show alarm statistics	Querying alarm statistics result.	User
show arp address	Showing the MAC address of host's maintenance network interface.	User
show arp entry	Showing the ARP table item	User
show baudrate	Showing the baud rate of serial port.	User

Command name	Function	Mode
show client	Showing the user's login condition.	User
show clock	Showing system time.	User
show cpu	Showing the CPU occupancy.	User
show data autosave setting	Showing the autosaving parameters of configuration data.	User
show data unsaved percent	Showing the saving progess of configuration data.	User
show device	Showing the equipment's status and information.	User
show dns status	Showing the configuration of DNS.	Privilege
show dsp-channel all	Showing the status of DSP channel.	Global Config
show environment	Showing the environmental variables (like temperature).	User
show ftpserver	Showing the login information of FTP server.	User
show h248stack	Showing the parameters of H248STACK.	User
show history	Showing history commands.	User
show iadms	Showing NMS information.	User
show infolevel cli	Showing the output level of command line information.	User
show infolevel nms	Showing the output level of NMS information.	User

Command name	Function	Mode
show infolevel syslog	Showing the output level of log host information.	User
show infoswitch cli	Showing the output switch of command line information.	User
show infoswitch nms	Showing the output switch of NMS information.	User
show infoswitch syslog	Showing the output switch of log host information.	User
show interface	Showing the LAN Switch interface.	LAN Switch
show ip route	Showing the system routing information.	Privilege
show language	Showing language information of host.	User
show log detailed	Showing a log in detail.	User
show log list	Showing the simple log list.	User
show loghost list	Showing the list of log hosts.	User
show lsw parameter	Showing the global configuration parameters of LAN Switch.	LAN Switch
show memory	Showing the device information.	Privilege
show mg attribute	Showing MG attribute configuration information.	User
show mg register-info	Showing MG interface registration key.	User
show mg software-parameter	Showing MG software parameter.	User

Command name	Function	Mode
show mg system-parameter	Showing the system parameters of the interface.	User
show mgcp para	Showing MGCP parameters.	User
show mgcp ver	Showing MGCP version.	User
show mgcpstatresult all	Showing signaling statistics result.	User
show mgcpstatresult portno	Showing signaling statistics result.	User
show mgcpstatresult telno	Showing signaling statistics result.	User
show mgcptrace all	Showing MGCP tracing information.	User
show mgcptrace portno	Showing MGCP tracing information.	User
show mgcptrace telno	Showing MGCP tracing information.	User
show mgringmode attribute	Showing the attributes of ringing mapping.	User
show mguser	Showing MG user information.	User / Global Config
show monitor-port	Showing the monitoring interface of LAN Switch.	LAN Switch
show multicast	Showing multicast configuration.	LAN Switch
show network parameter	Showing the parameters of host's maintenance interface.	User
show patch	Showing the patch information of CVP board.	User

Command name	Function	Mode
show port state	Showing the information of access user port.	user
show power	Showing the voltage and changing range.	Privilege
show progress backup	Showing the backup progress.	User
show progress load	Showing the loading progress.	User
show pstnport attribute	Showing the attributes of PSTN port.	Global Config
show pstnport kc	Showing the 16KC/12KC attribute of PSTN port.	Global Config
show qos	Showing QoS configuration.	LAN Switch
show rtp stat	Showing RTP statistics information.	User
show running-config	Showing the operation configuration of the system.	Privilege
show sntp status	Showing the configuration information of SNTP client.	Privilege
show spc	Showing the SPC.	User
show startup-config	Showing the startup configuration of the system.	Privilege
show tag	Showing the label of VLAN.	User
show temperature-limit	Showing the temperature threshold (Celsius).	User
show terminal timeout	Showing the timeout threshold for the terminal user to exit the system when timeouts.	User

Command name	Function	Mode
show terminal type	Showing terminal type.	User
show terminal user	Showing terminal user information.	User
show trace	Showing the related information of tracing module.	User
show trunk	Showing TRUNK configuration .	LAN Switch
show uplink	Showing uplink interface.	LAN Switch
show user defined-ring	Showing the user-defined ringing.	User
show version	Showing version information.	User
show vlan	Showing the VLAN of LAN Switch.	LAN Switch
shutdown	Closing the network interface of LAN Switch.	LAN Switch
slic reset	Resetting the SLIC chip.	Global Config
slic set	Configuring user attributes.	Advance
smart	Starting the interaction function.	User
sntp interval	Configuring the synchronous interval.	Global Config
sntp server	Configuring the server.	Global Config
sntp time-zone	Configuring the time zone.	Global Config
spc add	Adding an SPC.	Global Config
spc delete	Deleting an SPC.	Global Config
spc dsp-channel	Setting the attributes of DSP channel.	Global Config

Command name	Function	Mode
spc modify	Modifying an SPC.	Global Config
spc release	Releasing an SPC.	Global Config
speed	Setting the rate of the LAN Switch's network interface.	LAN Switch
startservice	Starting the service.	Global Config
system set aulaw	Setting DSP A/μ law.	Advance
T		
tag disable	Prohibiting the setting of VLAN label.	Global Config
tag enable	Enabling the setting of VLAN label.	Global Config
tag vlanid	Setting the VLAN label.	Global Config
telnet	Logging in the host via telnet mode.	User
temperature-limit	Setting the temperature threshold for starting the fan.	Global Config
terminal hold	Locking the user terminal.	User
terminal timeout	Enabling the function that when the terminal timeouts, it will exit from the system.	User
terminal type	Configuring the terminal type as ANSI/VT100.	User
timeout	Turning on the terminal timeout control switch.	User

Command name	Function	Mode
tos other	Setting the TOS of other media streams.	Global Config,MG Interface
tos voice	Setting the TOS of voice stream.	Global Config,MG Interface
tracert	Tracing the route to the destination.	User
U		
uplink	Setting a network interface of IAD as the uplink interface.	LAN Switch
user apdinfo	Modifying the user's appendix information.	Global Config
user disconnect	Terminating the connection of terminal user.	Privilege
user level	Modifying user level.	Global Config
user name	Modifying user name.	Global Config
user password	Modifying user's password.	Global Config
user reenter	Modifying the reenter times of the user.	Global Config
V		
vlan	Entering the VLAN mode of LAN Switch.	LAN Switch
W		
write	Saving the data immediately.	Privilege

Appendix B Acronyms

Acronym	Full name
3rd Party Server	Third Party Server
ADSL	Asymmetrical Digital Subscriber Loop
APU	ADSL Processing Unit
ATM	Asynchronous Transfer Mode
BHCA	Busy Hour Call Attempts
BOOTP	BOOT strap Protocol
CLI	Command Line Interface
CNG	Comfort Noise Generation
CSP	Control and Signal Processing board
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name Server
DOPRA	Distributed Object-oriented Programmable Real-time Architecture
DSL	Digital Subscriber Line
DSLAM	Digital Subscriber Line Access Multiplexer
DSP	Data Signal Processor
DTMF	Dual Tone Multi-Frequency
EC	Echo Cancellation
ETA	Ethernet Telephone Adapter

Acronym	Full name
FE	Fast Ethernet
FoIP	Fax over IP
FSK	Frequency Shift Keying
FTP	File Transfer Protocol
H.248	H.248/MECAGO protocol
IAD	Integrated Access Device
IADMS	Integrated Access Device Management System
MFC	Multi-Frequency Control
MGC	Media Gateway Controller
MGCP	Media Gateway Control Protocol
MGW	Media Gateway
MRS	Multimedia Resource Server
NGN	Next Generation Network
NMS	Network Management Station
OSS	Operating Support System
POTS	Plain Old Telephone Service
PS	Packed Switched
PSTN	Public Switched Telephone Network
QoS	Quality of Service
RTP	Real-time Transport Protocol
RTCP	Real-time Transfer Control Protocol
SCTP	Simple control transmission protocol

Acronym	Full name
SG	Signaling Gateway
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
SoftSwitch	SoftSwitch
TDM	Time Division Multiplexing
TFTP	Trivial File Transfer Protocol
TMG	Trunk Media Gateway
VAD	Voice Activity Detection
VDSL	Very-high-data-rate Digital Subscriber Line
VLAN	Virtual LAN
VoIP	Voice over IP
VPU	VDSL Processing Unit